Cybersecurity: Cloud, IoT, Wireless Networks

Ozalp Babaoglu

ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA

Cloud Computing

- Many organizations have an economic and technological incentive to move a portion or all of their IT operations to an Internet-connected infrastructure known as ***cloud computing***

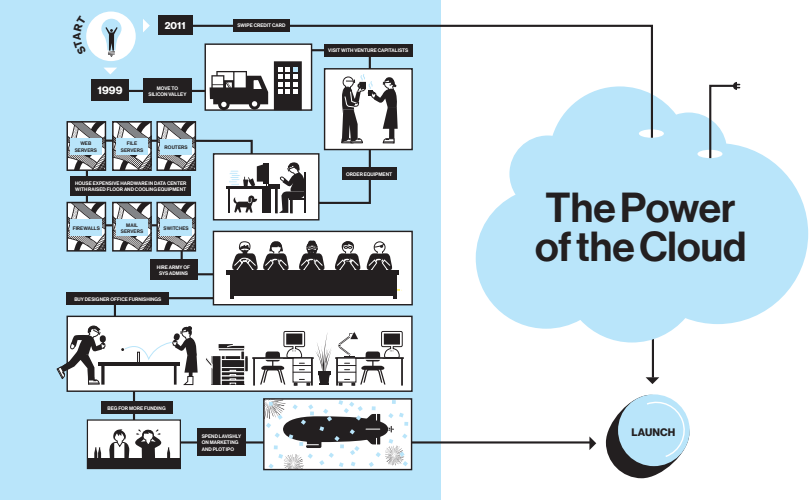
What is Cloud Computing?

- Clouds are the ***utilities*** for computing, just like conventional utilities for water, gas and electricity
- ***Cloud computing*** is a remote virtual pool of on-demand shared resources offering compute, storage, database and network services that can be rapidly deployed at scale
- ***Cloud computing*** is ***on-demand delivery*** of IT resources ***over the Internet*** with ***pay-as-you-go pricing***
- ***Cloud computing*** allows ***hardware*** to be treated (licensed, installed, configured, initialized, sized) just like ***software***

Why the Cloud?

- According to one estimate, by 2021 94% of all workloads and computing tasks will run in some form of cloud environment
- By adopting cloud computing, a business is transformed from a ***capital expenditure*** (CapEx) to ***operating expenditure*** (OpEx) model
- Allows an organization to focus on its ***core business*** instead of IT operations
- Business built on ***standardized***, ***up-to-date*** and consolidated IT
- Transfers ***investment***, ***risk*** and ***human resources*** to the cloud provider

Why Cloud Computing?



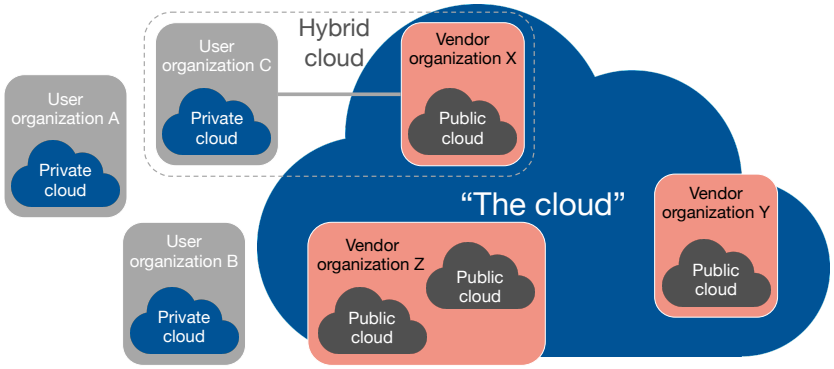
Cloud Computing Characteristics

- *Broad network access*: capabilities available over the network and accessed through standard mechanisms
- *On-demand self-service*: cloud customers can unilaterally provision computing resources without operator interaction
- *Rapid elasticity*: ability to dynamically expand and reduce resources according to demand
- *Shared infrastructure and resource pooling*: cloud provider's resources are pooled to service multiple cloud customers
- *Measured service*: transparent, fine-grained metering capability for billing — pay-per-usage

Cloud Deployment Models

- Based on the identities of the *provider* and *user* roles
  - Private cloud
  - Public cloud
  - Hybrid cloud

Cloud Deployment Models



Private Cloud

- Provider and users belong to the ***same organization***
- Services built to be ***compatible*** with generic cloud interfaces (private or public)
- No risk of ***vendor lock-in***
- ***Security*** and ***data protection*** in the hands of the user
- Costs for hardware, space and administration similar to ***on-premise non-cloud*** architectures
- Private cloud may be suitable for those applications that have strict ***security*** or ***regulatory compliances*** for data and computations needs or where the ***migration costs*** are excessive

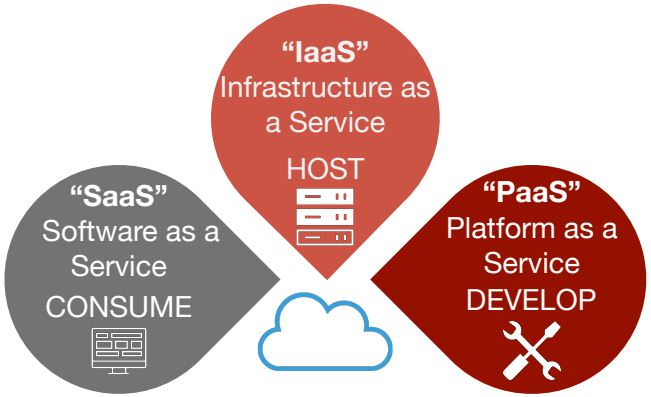
Public Cloud

- Provider and users belong to ***different organizations***
- Providers pursue ***commercial interests***
- Users ***do not invest*** in procurement, operation and maintenance of hardware
- Possible risk of ***vendor lock-in***
- ***Security*** and ***data protection*** guarantees largely dependent on the cloud provider and may be determining factors

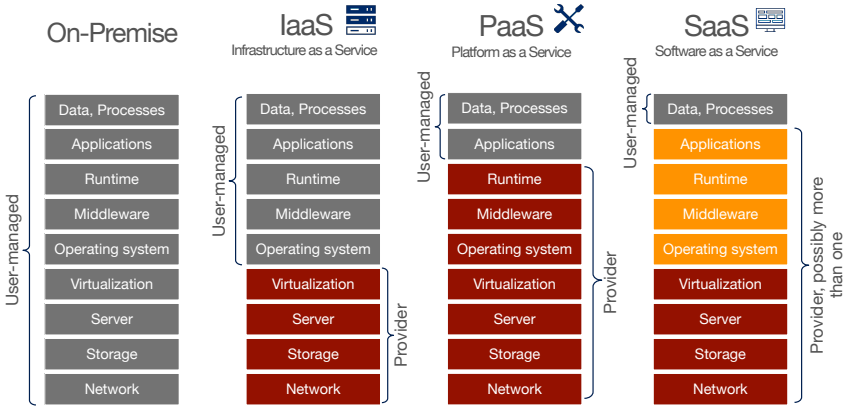
Hybrid Cloud

- Services from ***public and private clouds*** are used together within the ***same organization***
- Usage examples
  - Augment private cloud capacity with public clouds at times of ***peak demand***
  - Delegate certain functions such as ***data backup*** to public clouds
  - Leverage the ***security of private clouds*** together with the ***scale of public clouds***

Cloud Computing Models



IaaS vs. PaaS vs. SaaS



Security Issues for Cloud Computing

- Many of the security issues are similar to those for centralized data centers
- In cloud computing, responsibility for assuring security is shared among users, vendors and third-party providers
- Increased risk due to sharing vendor resources with other cloud users — users need to be protected from one another
- ***Virtualization*** is an effective technology for cloud infrastructures but buggy or incorrectly-configured visualization may allow user code to access sensitive portions of the cloud infrastructure or resources of other users

Cloud Computing Security Threats

- Abuse and malicious use of cloud computing
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking

Security Issues for Cloud Computing

- Cloud users need to be protected against the cloud provider, in particular against ***inadvertent data loss*** or ***data leakage***
- How does the cloud provider dispose of hardware that is retired or replaced?
- What are the political and legal implications of placing data at specific geographic locations?
- User-level encryption is an essential tool

Cloud Security

- There are ***conflicting views*** of security in a cloud computing setting
- Some believe that moving to a cloud ***frees*** an organization from all concerns related to computer security and ***eliminates*** a wide range of threats to their data
- By placing cloud security in the ***hands of experts*** (cloud provider), they believe that they are ***better protected*** than when using ***on-premise*** computing systems

Cloud Security

- Others believe that handing over data and programs to a cloud provider inherently ***reduces the security*** of an organization's IT operations
- Cloud users accustomed to operating ***inside a secure perimeter*** protected by corporate firewalls now have to extend their ***trust*** to the ***cloud service provider*** if they wish to benefit from the economical advantages of utility computing
- The transition away from a model where users have ***full control*** over where their sensitive information is ***stored*** and ***processed*** is a difficult one
- Virtually all surveys report that ***security is the top concern*** of cloud users

Cloud Computing Security Concerns

- Security concerns associated with cloud computing derive from ***two sources***:
  - Issues faced by ***cloud providers***,
  - Issues faced by ***their customers***
- Yet, the responsibility is ***shared***: the provider must ensure that their ***infrastructure is secure*** and that their clients' data and applications are protected, while users must take measures to ***fortify their applications***, use ***strong passwords*** and other ***authentication measures***

Cloud Computing Security Concerns Cloud Provider

- The ***cloud provider*** is responsible for
  - ***Physical security***: hardware infrastructure guarded against unauthorized access, theft, fires, floods, power outages and other catastrophic events
  - ***Personnel security***: security screening of potential employees, security awareness and training programs
  - ***Identity management***: integrate customer's identity management system with the provider's own infrastructure, use a federation or single-sign-on technology, biometric-based identification system
  - ***Up-to-date infrastructure***: hardware and software systems free of all known vulnerabilities

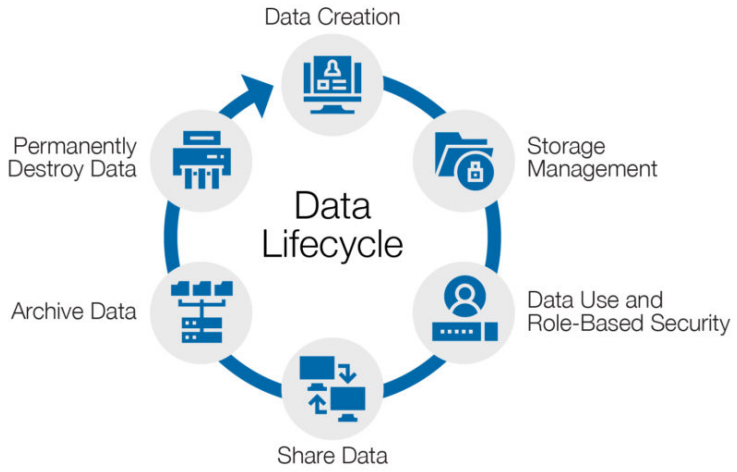
Cloud Computing Security Concerns Cloud Provider

- The ***cloud provider*** is also responsible for
  - ***Integrity*** and ***availability*** of ***user's data*** — user data is ***not corrupted*** and ***continues to be available*** despite unforeseen events (disk crashes)
  - ***Availability of services*** — cloud applications deployed by users ***continue to be available*** despite various ***disruptions*** (power outage, fire, flooding) and ***cyberattacks*** (denial-of-service attacks)

Cloud Computing Security Concerns Cloud Provider

- The ***pooled*** nature of the ***shared infrastructure*** resources that are necessary to facilitate elasticity can be a source for additional security concerns (data leakage)
- Software ***virtualization*** technologies that are necessary to provide the ***isolation*** among users introduce an ***additional layer*** that itself must be ***properly configured***, ***managed*** and ***secured***

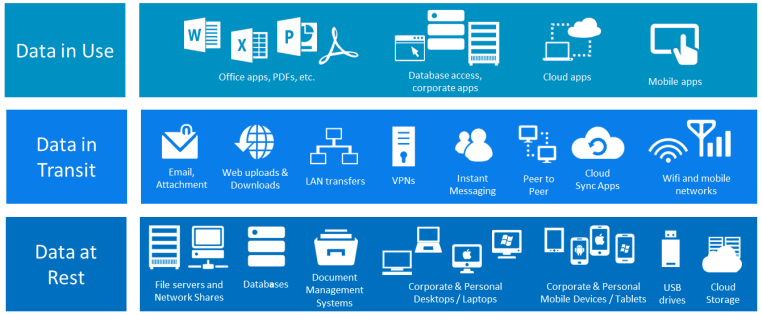
Data Lifecycle



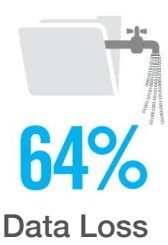
Data Lifecycle

- ***Control*** over the lifecycle of data in a cloud environment is difficult
- Typically, it is impossible for a user to
  - control where data is ***stored***,
  - control if and where it is ***backed up***,
  - determine if data that ***should have been deleted*** was ***actually deleted***
- When data is deleted, there is no guarantee that the media is ***wiped out*** and the next user is not able to recover confidential data
- Cloud providers often rely on ***backups***, typically performed without the user's knowledge or consent, to prevent accidental data loss

States of Data



Cloud Computing Security Concerns Cloud User



64%

Data Loss

62%

Data Confidentiality

Cloud Computing Security Concerns Cloud User

- ***Cloud users*** have several tools to preserve the ***confidentiality*** of their data and ***minimize risk of data loss*** in cloud settings
- Key technologies that can be deployed in isolation or in combination:
  - *Data encryption*
  - *Data replication*

Cloud Data Encryption

- Encryption of sensitive data is a critical defense against ***unauthorized access*** and ***data theft***
- Encrypted data—even if accessed or stolen —are ***useless*** to third parties without the encryption keys
- A ***cloud data encryption policy*** needs to answer:
  - ***What*** data needs encryption?
  - ***When*** does data need encryption?
  - ***Where*** should cloud encryption be deployed?
  - ***Who*** should hold the encryption keys?

Cloud Data Encryption

- *What* data needs encryption? Need to consider
  - Do the data fall under ***regulatory compliance requirements***, such as health records (HIPAA), financial data (PCI, SOX), privacy acts (GDPR), or other legal or contractual obligations?
  - Are the data ***personally identifiable*** information?
  - Do the data contain sensitive ***intellectual property***?
  - Are the data ***essential*** to the operation of the organization?

Cloud Data Encryption

- *When* does data need encryption?
  - Encrypting ***data at-rest*** — data saved on disk or other media — is ***essential***
  - Data that moves between the ***user organization*** and the ***cloud provider*** or ***between different clouds*** — ***data in-transit*** — is also vulnerable
  - Communication protocols such as ***SSL***, ***TLS***, ***IPSec***, ***virtual private network*** (VPN) should be used to secure data in-transit

Cloud Data Encryption

- *Where* should cloud encryption be deployed?
  - ***Client-Side Encryption*** — Encrypt data client-side before uploading them to the cloud
  - ***Server-Side Encryption*** — Request cloud provider to encrypt your data before saving them on disks in its data centers. Most major cloud providers offer data-at-rest encryption (Amazon S3 with AES-256)
  - ***Cloud Application Encryption*** — Many software-as-a-service (SaaS) application vendors provide de facto or optional encryption of data. Risk of vendor lock-in
  - ***Cloud Security Service Software Encryption*** — As a part of their protection services, third-party security software companies offer encryption technologies (***Gemalto SafeNet ProtectV***)

Cloud Data Encryption

- *Who* should hold the encryption keys?
  - Encryption keys can be ***managed*** either by the ***cloud provider*** or by the ***users***
  - Regulatory ***compliance considerations*** may come into factor
  - Regardless of who holds the keys, organizations should make certain that key access is through ***multi-factor authentication*** and that key storage is itself secure and backed
  - Moreover, organizations should keep their keys on storage media ***separate*** from their data

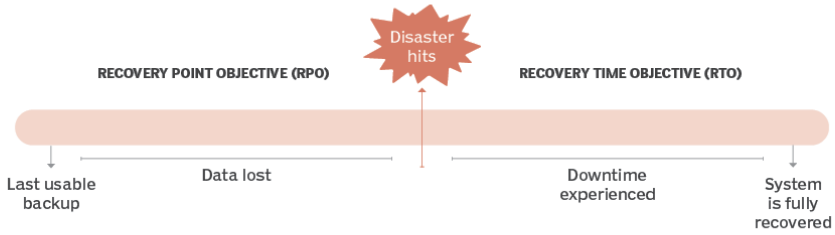
Cloud Data Encryption

- Sensitive data is ***safe while at-rest***, provided that it is encrypted with strong encryption
- To be ***processed***, encrypted data must be ***decrypted*** and this opens a ***window of vulnerability***
- Processing data in its ***encrypted state*** without decrypting is a long-time goal of cryptography and several attempts such as ***homomorphic encryption***, ***searchable symmetric encryption*** and ***order-preserving encryption*** exist

Disaster Recovery

- ***Recovery Time Objective*** (RTO) is the duration of time within which a business process ***must be restored*** after a disaster in order to avoid unacceptable consequences associated with a break in continuity
- ***Recovery Point Objective*** (RPO) describes the interval of time that might pass between your last data backup and a disaster before the ***quantity of data lost*** during that period causes ***serious damage*** to your business

Disaster Recovery



Data Replication Strategies

- ***Single copy*** — no replication
- ***Periodic backups*** — a backup is like a replica but limited to ***disaster recovery*** and not suitable for ***normal access***
- ***Independent copies*** — any copy can be ***read*** (for increased throughput) but ***not written***. Not suitable if data can change (be ***written***)
- ***Master-Slave*** — any copy can be ***read***, but writes limited to a ***master*** that assumes the responsibility to ***propagate*** the changes to slaves
- ***Fully distributed*** — any copy can be ***read***, any copy can be ***written*** subject to different consistency obligations

Data Consistency Models

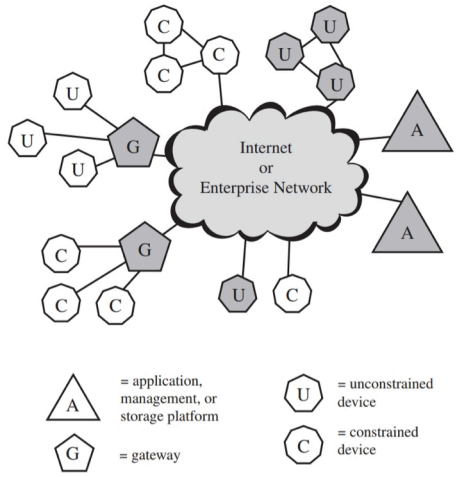
- How should the replicated version of data behave when compared to its non-replicated counterpart?
  - *Strict consistency* — all updates to an item are seen by all copies in the same order (copies always return the value of the last update)
  - *Sequential consistency* — updates to an item by any given writer is seen by all copies in the same order
  - *Causal consistency* — only updates that are causally related are seen by all copies in the same order
  - *Eventual consistency* — if no new updates are made to a given data item, eventually all copies of that item will return the last update value

From Cloud Computing to Internet of Things

- *Edge*: extremity of a typical enterprise network of IoT-enabled devices — sensors, actuators (millions)
- *Fog*: computing devices close to the edge of the IoT network to process the large amounts of volumes of generated data (tens of thousands)
- *Core*: backbone network connecting geographically dispersed fog networks (thousands)
- *Cloud*: provides the storage and processing capabilities for the massive amounts of aggregated data originating at the edge, hosts applications to interact with and manage the IoT-enabled devices (hundreds)

IoT Security

- Elements of IoT security (shaded regions include security features):



IoT Security

- Typically, gateways implement secure functions, such as TLS and IPsec
- *Unconstrained* devices may or may not implement some security capability
- *Constrained* devices generally have limited or no security features
- *Gateway* devices can provide secure communication between the gateway and the devices at the center
- Unconstrained devices can communicate directly with the center and support security functions
- Constrained devices that are not connected to gateways have no secure communications with central devices

IoT and Embedded Systems

- IoT devices that are embedded systems (video surveillance cameras, home alarms, baby monitors, thermostats, etc.) represent increased security risks
- Embedded devices are riddled with vulnerabilities and there is no good way to patch them
- Chip manufacturers have strong incentives to produce their product as quickly and cheaply as possible
- Device manufacturers choose a chip based on price and features and not on the ease of firmware updates
- The end user may have no means of patching the system and, if so, little information about when and how to patch
- The result is hundreds of millions of Internet-connected devices that are vulnerable to attack

IoT Security

- Key development in IoT security is ITU-T Recommendation Y.2067 (*Common Requirements and Capabilities of a Gateway for Internet of Things Applications*, June 2014) which defines specific security functions:
  - Support identification of each access to the connected devices
  - Support mutual or one-way authentication with devices
  - Support mutual authentication with applications
  - Support the security of the data that are stored in devices and the gateway
  - Support mechanisms to protect privacy for devices and the gateway
  - Support self-diagnosis and self-repair as well as remote maintenance
  - Support firmware and software update

Security of Wireless Networks

- Wireless networks present increased security risks because
  - Unlike a wired LAN which requires a physical connection, with a wireless LAN any station within radio range of other devices can transmit and receive
  - Communication is typically through *broadcasting* (not point-to-point) which is more susceptible to eavesdropping and jamming
  - They are more vulnerable to active attacks
  - Wireless devices are often mobile
  - Wireless devices often have limited resources
  - Wireless devices often easier to access physically

Wireless Network Standards — IEEE 802.11

- IEEE 802: a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990 the IEEE 802.11 working group is formed to develop a protocol and transmission specifications for wireless LANs (WLANs)
- 802.11b — the first 802.11 standard to gain broad industry acceptance
- In 1999 the "Wi-Fi Alliance" formed to hold the "Wi-Fi" trademark
  - The term used for certified 802.11b products
  - Extended to 802.11g, 802.11ac, 802.11n products

Wireless LAN Security Standards

- For privacy, the original 802.11 defined the *Wired Equivalent Privacy* (WEP) algorithm which was shown to contain major weaknesses
- The Wi-Fi Alliance defined the *Wi-Fi Protected Access* (WPA) to address the insecurities in WEP
- WEP and WAP based on the RC4 stream cipher
- 802.11i task group charged with developing a set of capabilities to address the WLAN security issues
- The final form of the 802.11i standard is WPA2 also known as *Robust Security Network* (RSN)
- RSN based on the AES block cipher

IEEE 802.11i Services

- ***Authentication***: provides mutual authentication between a user and an Authentication Server and generates temporary keys to be used between the client and the AP over the wireless link
- ***Access Control***: enforces the use of the authentication function, routes the messages properly, and facilitates key exchange
- ***Privacy with message integrity***: MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered

Wireless Network Threats

- ***Accidental association*** — WLANs in close proximity
- ***Malicious association*** — fake access points
- ***Ad hoc networks*** — p2p networks between devices
- ***Nontraditional networks*** — Bluetooth or other technologies
- ***Identity theft*** — MAC spoofing
- ***Man-in-the-middle attack*** — between user and access point
- ***Denial of service*** — particularly easy to direct wireless messages to a target
- ***Network injection*** — access points that are exposed to routing protocol or network management messages
- ***Sniffing*** — particularly easy to eavesdrop on packets

Securing Wireless Network

- Principal threats — eavesdropping, altering, injection, disruption
- Signal hiding techniques
  - Turn off SSID broadcasting by access point
  - Assign cryptic names to SSID
  - Reduce signal strength
  - Locate access points inside buildings, away from windows and exterior walls

Securing Wireless Network

- Other techniques
  - Use encryption
  - Use antivirus, anti spyware software and firewall
  - Change your access point's default admin password
  - Turn on MAC filtering in the access point to allow only specific computers to access the wireless network

Securing Wireless Access Points

- Limiting access to the network
- *Port-Based Network Access Control* (PNAC) provides an authentication mechanism to devices wishing to attach to a LAN
- 802.1X is an IEEE standard for PNAC based on the *Extensible Authentication Protocol* (EAP)
- 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Sniffing – Commercial products

riverbed

Products / SteelCentral / Riverbed AirPcap

RIVERBED AIRPCAP

AirPcap Adapter for Microsoft Windows

Wireless traffic packet capture

Capture 802.11 WLAN packets for rapid, comprehensive analysis with your favorite packet-analysis software. This is the only Microsoft Windows-based wireless packet capture device fully integrated with Wireshark and Riverbed® SteelCentral™ Packet Analyzer. Choose among three affordable, easy-to-deploy versions: AirPcap Classic, AirPcap Tx, and AirPcap Nx.

Select your AirPcap Model

Sniffing – Commercial products

Riverbed Technology Product Catalog

	Product Name	Price	Buy Now
PA	SteelCentral™ Packet Analyzer Personal Edition	$695.00	Buy Now
PA	SteelCentral™ Packet Analyzer PE to Enterprise Upgrade	$2,749.00	Buy Now
AirPcap Tx	AirPcap Tx: USB 802.11b/g Adapter (capture + injection)	$298.00	Buy Now
	AirPcap Tx USB 802.11b/g Three-Pack (capture + injection)	$894.00	Buy Now
AirPcap Nx	AirPcap Nx: USB 802.11a/b/g/n Adapter (capture + injection)	$698.00	Buy Now
	AirPcap Nx USB 802.11a/b/g/n Three-Pack (capture + injection)	$2,094.00	Buy Now

Sniffing — Mac OS X Commands and Tools

- Scan available networks

```
cd /System/Library/PrivateFrameworks/
Apple80211.framework/Versions/Current/Resources
./airport en0 --scan
```

- "Wireless Diagnostics" tool (Option-click WiFi icon in menu)
- Builtin "Packet Sniffer"

```
cd ~/Desktop
/usr/sbin/tcpdump -i en0 -w xxx
/usr/local/bin/wireshark xxx
```


Risks of "Open Networks"

- "Open networks" allow access without supplying a password
- Render access "convenient" but at great risk, particularly in public networks
- Wi-Fi password is used to encrypt data between client and access point
- Without it, data is transmitted in clear, making sniffing trivial

Google Street View Scandal

- 15 May 2010, *The Guardian*: "Google admits collecting Wi-Fi data through Street View cars"
  - In a post on its European Public Policy blog on 27 April, Google stated that it does gather wi-fi network names (SSIDs) and identifiers (Mac addresses) for devices like network routers, it has been mistakenly collecting samples of payload data from open wi-fi networks (in addition to SSIDs and Mac addresses for devices like network routers)

Public Wi-Fi Usage Advice

- Don't use public Wi-Fi to shop online, log in to your financial institution, or access other sensitive sites — ever
- Use a Virtual Private Network
- Implement two-factor authentication when logging into sensitive sites
- Only visit websites with HTTPS encryption
- Turn off file sharing
- Turn off automatic Wi-Fi connectivity feature
- Monitor your Bluetooth connection when in public places to ensure others are not intercepting your transfer of data