AIRLOCK

Web Application Security

Erwin Huber
Head of Research & Development
Web Application Security

ergon
smart people *smart software*

AIRLOCK

Web Application Security Unit

Strong Focus on Web Application Security since 1996
− Protection of Web Applications against attacks and manipulation
− Access Control, Identity Management and Single Sign On for Web environments

17 Employees

Top Class Customer References
− Over 200 customers with more than 500 installations in 8 countries
− 9 out of 10 banks in Switzerland protect their e-Banking with Airlock

Indirect Sales Model / direct touch

SAP
GLOBAL
SECURITY
ALLIANCE

vmware° | technology alliance **PARTNER**

Business Partner
hp ®
invent

PCI SECURITY
VENDOR ALLIANCE

**SWISS
TECHNOLOGY**
AWARD

AIRLOCK

Mega Trend: Web Applications

− e-banking (starts by end of the nineties)
− e-Shops
− e-Government

− Intranet Portals (emloyees)
− Extranet Portals (Partner)

− Web 2.0 Applications / Social Network
− Collaboration (MS Sharepoint etc)

→ Massive savings, growing customer satisfaction, more visibility

→ So far so good – but what is with security

AIRLOCK

Motivation

Today's Application Level Attacks are targeted and motivated by
− Data theft (criminally, commercially)
− Espionage
− Reputation damage
− Malware Deployment (Spam, Botnets)
− Identity Theft
− Denial of Service

!! SILENT ATTACK !!

Web Applications & Web Services are the most attractive target as they represent an electronic interface to data

Many people say «We never had such a problem» – well.... how do you know?
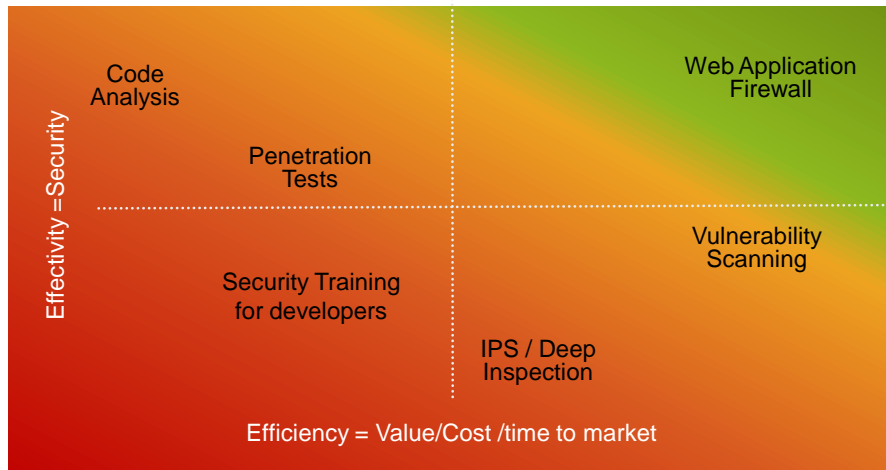*Application level data theft is not recognized in most cases!*

AIRLOCK

How to make web applications more secure?
There is no Silver Bullet

Web application security is always a combination of instruments
Goal: **Achieve maximum security with reasonable effort ($)**

AIRLOCK

Key Criteria for Application Security

WHOM are we dealing with?
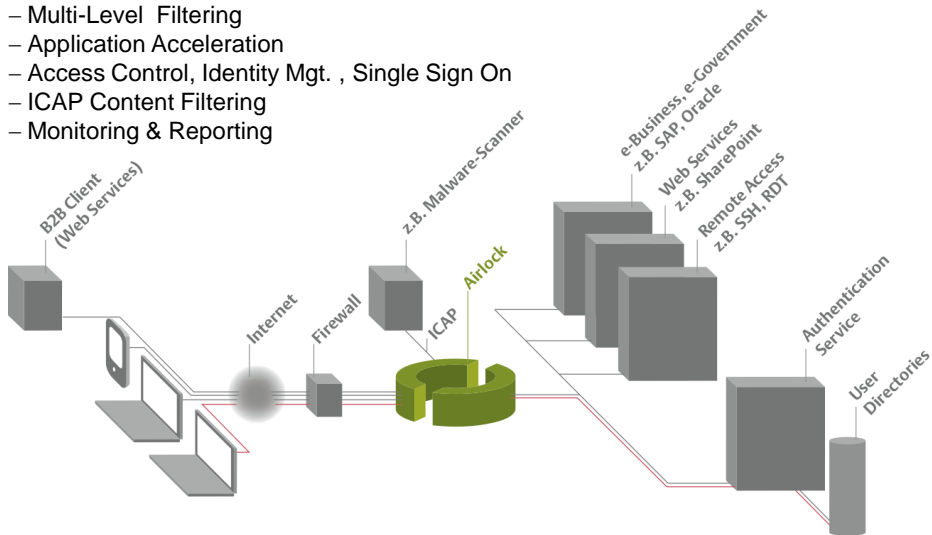
Access Control

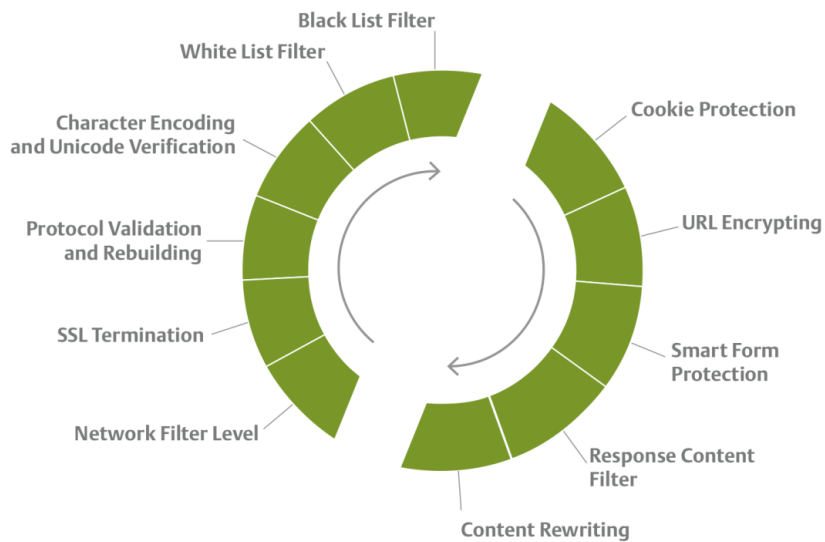WHAT are we dealing with?

Filtering

3

AIRLOCK

Strategic Web Entry Solution

- PCI-DSS Compliance
- Multi-Level Filtering
- Application Acceleration
- Access Control, Identity Mgt. , Single Sign On
- ICAP Content Filtering
- Monitoring & Reporting

AIRLOCK

Multi-Level Filtering

AIRLOCK
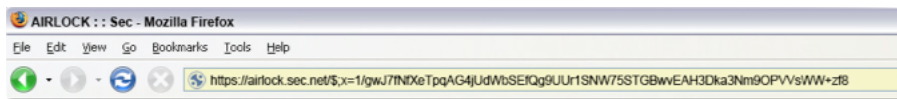
Dynamic Whitelisting Technologies

URL Encryption
– Effective protection against forceful browsing
– URLs and parameters 100% protected
– Topology and technology hiding
– Dynamic, no static configuration

Smart Form Protection
– Cryptographic protection of HTML forms
– Only valid inputs allowed
– Automatic protection of hidden fields, selections, etc
– Dynamic, no static configuration

Cookie Protection
– Cryptographic protection of application cookies
– Only valid cookies accepted
– Privacy & Integrity
– Dynamic, no static configuration
– Local cookie store

AIRLOCK : : Sec - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://airlock.sec.net/$;x=1/gwJ7fNfXeTpqAG4jUdWbSEfQg9UUr1SNW75STGBwvEAH3Dka3Nm9OPVVsWW+zf8

Application dynamically defines valid URLs, parameters and values.
Airlock enforces valid usage!

AIRLOCK

Cookie Protection
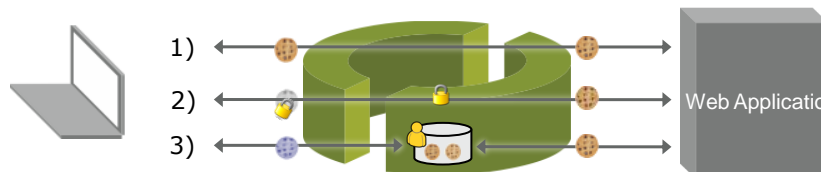
Pass-through (not protected)
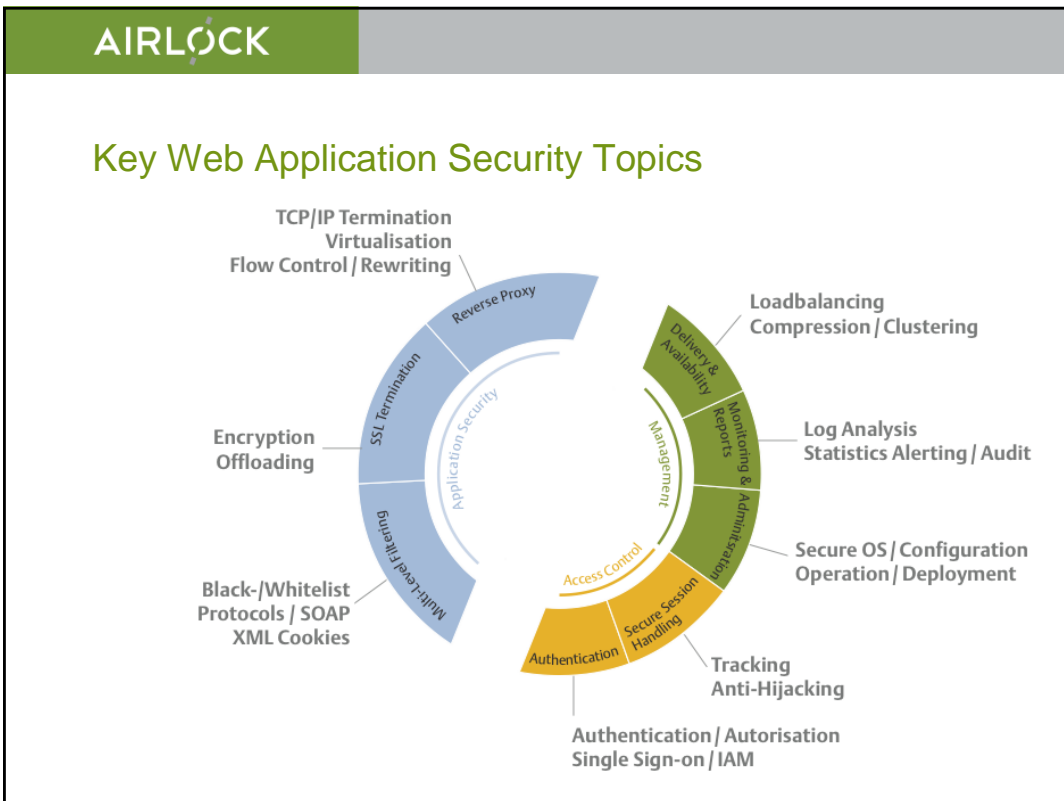– conventional, cookie may be read and manipulated in browser
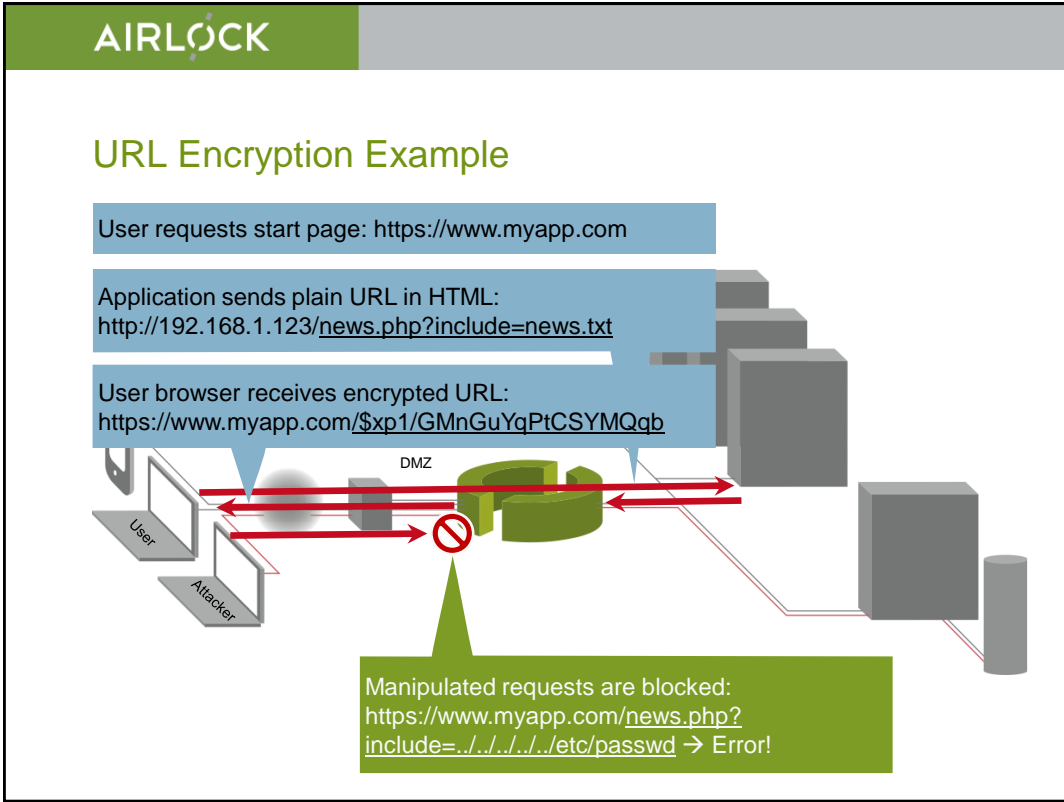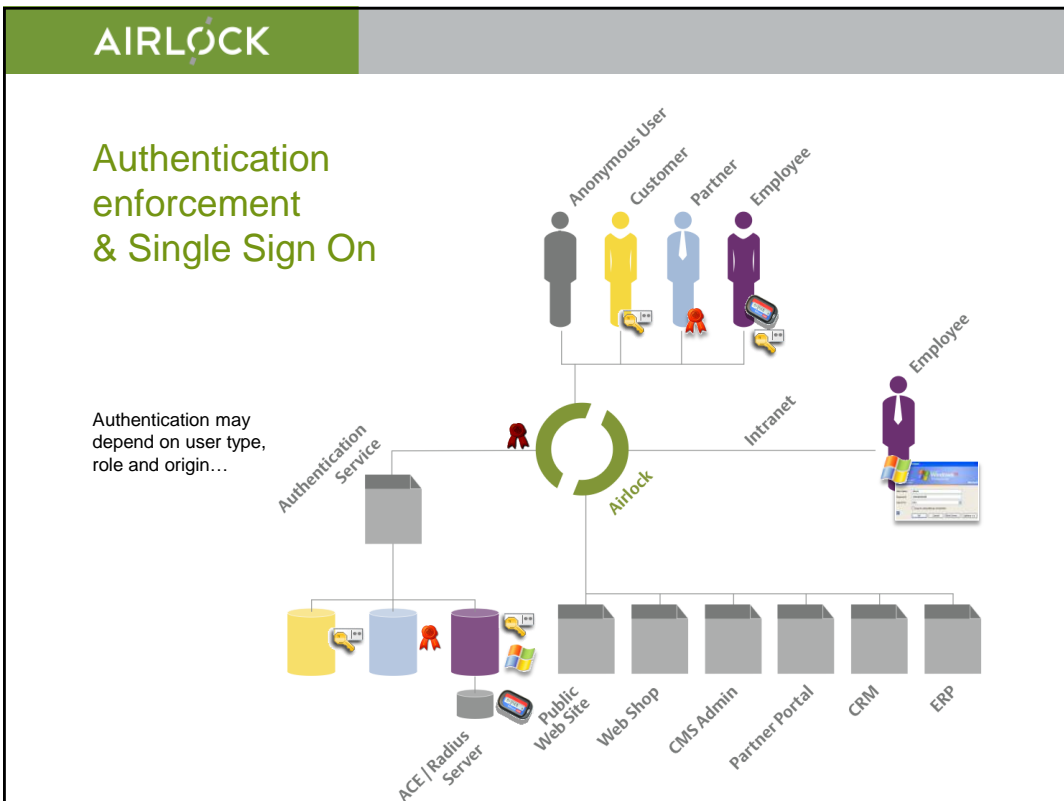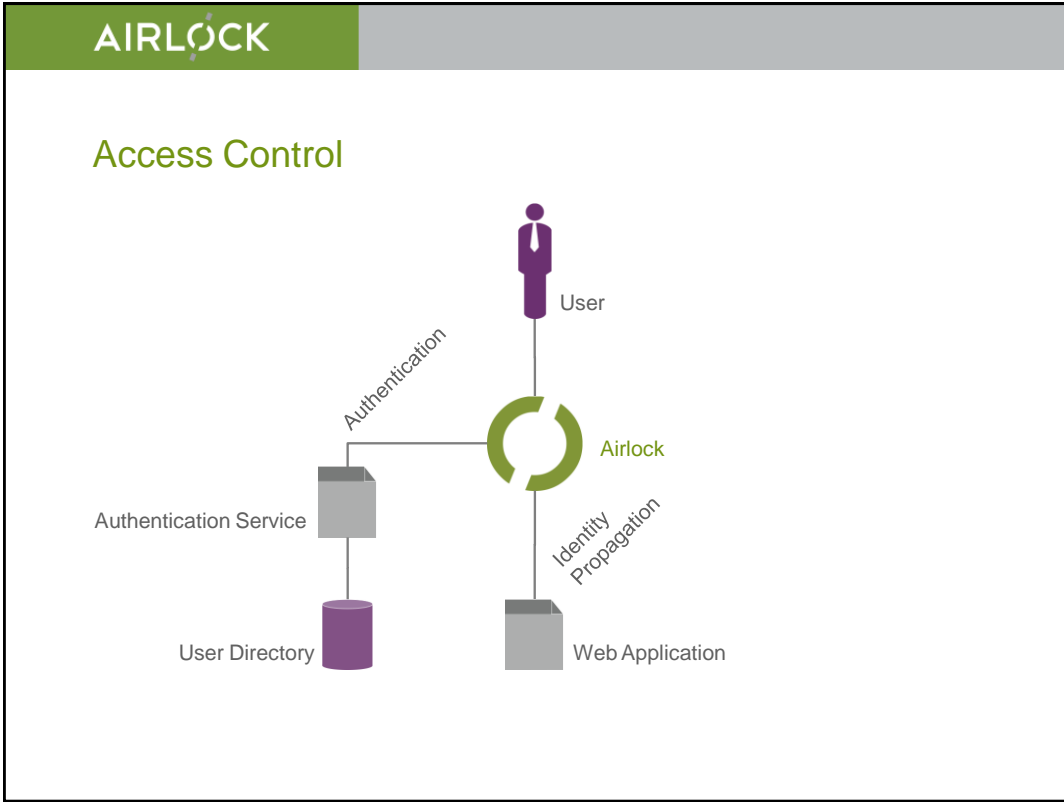– Same as without airlock

Encrypt
– airlock encrypts cookie before sending it to the browser
– Cookie not forgeable because a valid encryption is required

Store
– Cookies are not sent to browser but held in the user session on airlock
– airlock needs its own session tracking (cookie or SSL session)

AIRLOCK

URL Encryption Example

User requests start page: https://www.myapp.com

Application sends plain URL in HTML:
http://192.168.1.123/news.php?include=news.txt

User browser receives encrypted URL:
https://www.myapp.com/$xp1/GMnGuYqPtCSYMQqb

DMZ

User

Attacker

Manipulated requests are blocked:
https://www.myapp.com/news.php?
include=../../../../../etc/passwd → Error!

AIRLOCK

Key Web Application Security Topics

TCP/IP Termination
Virtualisation
Flow Control / Rewriting

Reverse Proxy

Loadbalancing
Compression / Clustering

Delivery & Availability

SSL Termination

Application Security

Monitoring & Reports

Management

Log Analysis
Statistics Alerting / Audit

Encryption
Offloading

Administration

Secure OS / Configuration
Operation / Deployment

Multi-Level Filtering

Access Control

Black-/Whitelist
Protocols / SOAP
XML Cookies

Authentication

Secure Session Handling

Tracking
Anti-Hijacking

Authentication / Autorisation
Single Sign-on / IAM

AIRLOCK

Access Control

User

Authentication

Airlock

Authentication Service

Identity
Propagation

User Directory

Web Application

AIRLOCK

Authentication enforcement & Single Sign On

Authentication may depend on user type, role and origin…

Anonymous User
Customer
Partner
Employee

Employee

Authentication
Service

Intranet

Airlock

ACE | Radius
Server
Public
Web Site
Web Shop
CMS Admin
Partner Portal
CRM
ERP

AIRLOCK

Airlock Secure Active Sync

Authentication via SSL client certificate before the access onto Exchange servers

Active-Sync specific whitelist-rules

Device-independent:
- Windows Mobile
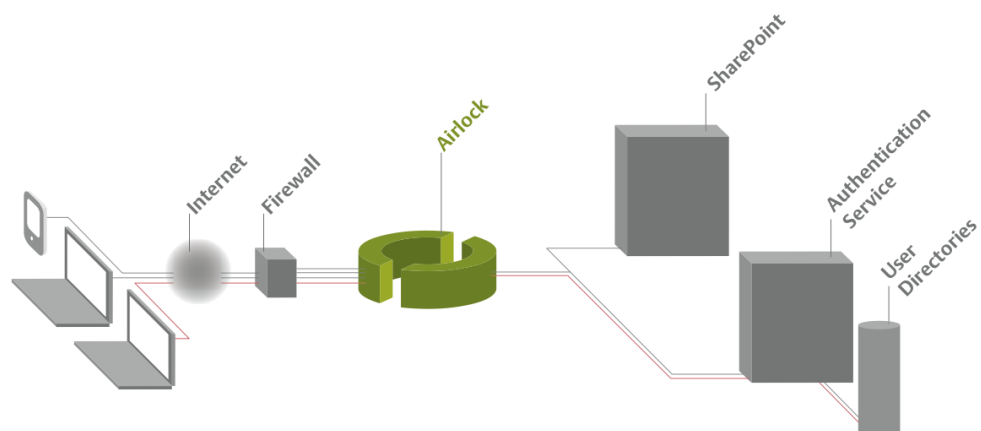- Nokia N-Series
- Apple iPhone

Supported
- Push Email
- Calendar & contacts synchronisation
- Enforcement of data erasing if client is lost or subject to brute force
- Policy enforcement for e.g. device password

Microsoft®
Exchange

AIRLOCK

Airlock SharePoint Integration

Internet Firewall Airlock SharePoint Authentication Service User Directories

AIRLOCK

Your Choice: Airlock benefits!

- Leading Web application firewall in central Europe

- Competent and trusted product development in Switzerland

- Unique and unmatched combination of authentication enforcement, filtering and high security platform

- Only WAF solution with real dynamic whitelisting
  (much easier to manage, less operational costs, less
  application dependencies)

- Rapid Web-Security Compliance (e.g. PCI-DSS, Certified Secure Web)

AIRLOCK

Thank you!

https://techzone.ergon.ch/url-encryption

erwin.huber@ergon.ch