PANEL SECURWARE/DEPEND

Security and Trust in IoT-based Complex Systems
Today’s Panelists

- **Moderator:**
  Petre Dini, Concordia University, Canada || China Space Agency Center, China

- **Panelists:**
  Giray Kömürcü, Tubitak-Bilgem, Turkey
  Possible cheap security solutions on Internet of Things based on Physical Uncloneable Functions

  Vito Santarcangelo, Centro Studi S.r.l., Italia
  ISO 27001: 2013 for the development of security policies in IoT“; "IoT Security: The Shodan case"

  Curtis Busby-Earle, The University of the West Indies at Mona, Jamaica

  security concerns related to the emergent behaviours that would result from the unification the many and varied "components" of an IoT

  Vladimir Muliukha, Peter the Great St. Petersburg Polytechnic University, Russia
  vision of security issues of distributed systems; on the difference between "Confidentiality" and "Security"
Thanks!

Qs & As

WWW.IARIA.ORG
Securware 2015

Security and Trust in IoT-based Complex Systems

Curtis Busby-Earle, PhD
Internet of Things?

- Ubiquitous Computing
  - “...to unify the multiple interfaces to disparate resources loosely connected on a variety of networking mediums”

- Networking
  - protocols, devices, apps, cost
  - opened up the possibility of computer technology receding into the environment

Curtis Busby-Earle, PhD
Emergent Behaviour

● When combined, how do/will these “systems” behave?

● Must consider
  ○ security and usability
  ○ security and performance
  ○ security and interoperability/interference
  ○ security and privacy
  ○ security and social interactions (e.g. networks of PNoTs)
  ○ …
Port existing solutions?

- Firewall on every device?
- IDS on every device?
- Anti-malware on every device?
- Challenge response protocol implemented on every device?
- Encrypt/decrypt communication on every device?
- ...

Maybe, not so practical!

Curtis Busby-Earle, PhD
New approaches

• Must develop new approaches
  ○ more dynamic - must be able to deal with unknown, emergent behaviour
    ■ very difficult!

• Must truly build security *into* “things”
What’s next?

Your thoughts and ideas!

Curtis Busby-Earle, PhD
PANEL

IoT Security: The Shodan case

Vito Santarcangelo
Applied Research Engineer
Centro Studi S.r.l.

Centro Studi
Process Development & Applied Research

Venice, 26 August 2015
The IoT Scenario

- IoT is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with other connected devices.

- Examples of applications: Media, Surveillance, Building and home automation, Environmental monitoring, Infrastructure management, Energy management, Medical and healthcare systems.
Common Problems

A common network… common Problems!

Examples of security problems for IoT devices:

- USE OF DIRECT DEVICE PORTFORWARDING INSTEAD OF VPN ACCESS

- DIRECT REMOTE ACCESS (eg. Synology QuickConnect) INSTEAD OF VPN ACCESS

- USE OF DEFAULT USER AND PASSWORD CREDENTIALS

- Firmware’s BUGS (VERSION OUTDATED)
THE SHODAN CASE

- Google finds web sites - Shodan finds devices

e.g.

Search by features (e.g. OpenSSL version, OS)

Search by vendor
SHODAN

www.shodan.io

The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
Heartbleed is a bug present in OpenSSL versions 1.0.1 through 1.0.1f.
EXAMPLE OF SEARCH by vendor
SHODAN MAP
default password - Finds results with "default password" in the banner; the named defaults might work!
Router w/ Default Info - Routers that give their default username/password as admin/1234 in their banner.
webcamxp - one of the best dorks for ip cameras/webcams
D-Link Internet Camera - D-Link Internet Camera DCS-5300 series, without authentication.
IPads - IPads. Think different. Think no security.
cisco-ios last-modified - Finds Cisco-IOS results that do not require any authentication ;-) 
Snom VOIP phones with no authentication - A list of Snom phone management interface without authentication
Anonymous access granted - title says it all, mostly FTP servers would be visible
iOmega NAS Devices (no passwords) - A bunch of external hard drives without passwords attached to the interbuttz
EXAMPLES
SOLUTIONS

- Robust authentication credentials
- Firmware upgrade
- Use of OTP (One Time Password) Auth Method
- Security devices as Firewall, IDS and IPS
- VPN Networks
REFERENCES

For more information and dataset visit

http://www.researchgate.net/profile/Vito_Santarcangelo

Thanks for the attention!
ISO 27001:2013 for the development of security policies in IoT

Vito Santarcangelo
Applied Research Engineer
Centro Studi S.r.l.

Venice, 26 August 2015
IoT is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with other connected devices.
ISO 27001:2013 AND ANNEX A

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

ISO 27000 : Fundamentals and vocabulary

ISO 27001 : ISMS Requirements (normative)

ISO 27002 : ISMS Code of practice (guide)

ISO 27001’s Annex A
list of 114 controls /best practices
(35 control objectives, 14 key points from A.5 to A.18)
POLICIES FOR IoT

A.6 Organization of information security

A.6.2 Mobile devices and teleworking (to enable connection from mobile devices through teleworking infrastructure)

A.9 Access control

A.9.1 Business requirements of access control (to establish an access control policy to limit access to information)
A.9.2 User access management (to prevent unauthorized access to systems and services)
A.9.3 User responsibilities (user must safeguard their authentication information)
A.9.4 System and application access control (secure log-on procedures)

A.10 Cryptography

A.10.1 Cryptographic controls (to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information)
POSSIBLE IMPLEMENTATION

1) Robust authentication and periodically change of the credential
2) Use of OTP Authentication
3) Access based on IP Filtering
4) Record the generality of connected users and IP
5) Use of VPN Network
POLICIES FOR IoT

A.12 Operation security

A.12.2 Protection from malware (controls against malware)

A.13 Communication security

A.13.1 Network security management (network controls, security of network services, segregation in networks)
A.13.2 Information transfer (information transfer policies and procedures)
POSSIBLE IMPLEMENTATION

1) **Use VLANs**
2) **Install Firewall, Antivirus Gateway**
3) **Install IDS and IPS (intrusion prevention system)**
REFERENCES

For more information and dataset visit

http://www.researchgate.net/profile/Vito_Santarcangelo

Thanks for the attention!
Static and Dynamic Aspects of Distributed Cloud Security Systems

Vladimir Muliukha

Institute of Applied Mathematics and Mechanics,
Telematics Department
“subject” buy a ticket and access to “object”, but constantly watched by an “object curator”
Access relationship and resources merges together by access **policy semantics**: user (or subject) may try to have access to resource and policy “curator” control “behavior” of the subject and feedback replay from the object.

Access control policy can be divided into **static** and **dynamic** parts:

- **Static** part (known as mandatory) set by administrator;
- **Dynamic** one is **content** (semantic, behavior, data) dependent.

To merge static and dynamic aspects of access policy firewall in cloud environment should have **self-aware** feature and provide security as a **new kind of cloud service**.
Proposed Security Conveyor Architecture

- Remote users/resources
- Static Packet Filtering
- Dynamic Security Monitor
- "Stealth" filtration
- real-time update for each connection
- Access Policy Description
- Algebra of Filtering Rules Optimization
- Informational Virtual Connections
- Set of Firewall Rules
- Transport Virtual Connections
- Local users/resources
- IMR
- Local DB
- Protocol State Machine
Dynamic Security Monitor

Security policy semantics form invariant essence of access rules transformations (3,4,5,6).
Implementation: Hypervisor with Stealth Firewall

- domS is a firewall virtual machine
- Firewall is “stealth” for object (interfaces have no IP or MAC addresses)
- Firewall controls VC traffic (between VMs and from external resources)
- domS is using Hypervisors resources – cores/memory
- domS doesn’t require to change cloud or VM configuration. The only change is hypervisor network subsystem.

Advances: firewall configuration (hardware and software) is scaled according to current cloud state.
Hypervisor provides VFW services
Private cloud protected by FW
Dynamic access policy forms by FSCS and replicated to all firewalls
Security Service: Trade-off between Confidentiality and Availability

Confidentiality  Availability
Is HIGHER SECURITY In IoT With PHYSICAL UNCLONABLE FUNCTIONS POSSIBLE?

Giray Kömürçü
What is PUF?

- Physical Unclonable Function
- Unique capability of generating chip specific signatures
- Uncontrollable components in the manufacture process
  - Gate delays, wire delays, threshold voltages...
- Applicable for both ASIC and FPGA
- Different types of PUFs have been developed
  - Ring Oscillator PUF, Arbiter PUF, SRAM PUF, Glitch PUF etc.
- Uniqueness, Robustness, Unpredictability and Unclonability is the key features
- Low cost solutions
Ring Oscillator PUF
- Depends on the delay differences of identical structures
- Oscillation frequencies of 2 identical ring oscillators are compared

- ‘1’ is generated if freq(RO1) < freq(RO2)
- ‘0’ is generated if freq(RO1) > freq(RO2)
Usage Areas

- **IP protection**
  - Design theft through FPGA bitstream duplication
- **Secret Key Generation and Storage**
  - Eliminates the problem of Secret Key Sharing and Non-Volatile-Memory requirements
- **IC Identification and Authentication**
  - ID generation, authentication through Challenge-Response Pairs
Outputs are generated depending on the inputs to the system, as well as device mismatches.

- Used in authentication
- Some PUF types support CRP property
- Conventional RO-PUFs support limited number of CRPs
Authentication Using PUFs

- Authenticity of devices is important in IoT

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>00101101</td>
<td>110101</td>
</tr>
<tr>
<td>10110110</td>
<td>001011</td>
</tr>
<tr>
<td>01101011</td>
<td>101000</td>
</tr>
<tr>
<td>10001101</td>
<td>111001</td>
</tr>
</tbody>
</table>

Device A Database
IoT is vulnerable against attackers since it is an open environment.

- Authentic devices may be replaced with replicas
  - Secure authentication is critical
- Secret Key sharing may threaten the system security
  - Especially if periodic key deployment is required
- PUFs can help improving the system security with low additional cost
PUFs have the unique capability of generating chip specific signatures

- PUFs can be used to supply higher security for low cost in several areas including IoT