IoT Security for Critical Information Infrastructures

Andrey Tikhonov
THE SCALE OF EVENTS

World Economic Forum 2018

Top-10 IoT Security Targets
IoT and Critical Information Infrastructures
EVOLUTION OF SECURITY IN "SMART" SYSTEMS

CYBER-PHYSICAL SYSTEMS

SECURITY DOMAINS
EVOLUTION OF “TRUST NETWORKS”

CENTRALISED

INSTITUTIONAL
(AUTHORITY)

DECENTRALISED

INTERPERSONAL
(SOCIAL CONTROL)

DISTRIBUTED

BLOCKCHAIN
(AUTONOMOUS)
The State emphasises the protection of Key Information Infrastructure in public communications and information services, i.e. telecommunications, energy, finance, transportation, water conservation, public services and e-governance, as well as other critical information infrastructure that could cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked (Articles 31, 187).
HOW WE FIT WITH THE REGULATORY TREND

- Priorities to the **nationally certified** technologies and solutions or even direct requirements for their use in CII Protection

- Cyberspace and **CII sovereignty** (cross-border data transmission rules + in-house control of key technologies)

- **General auditing and supervising the protection of CII**, from the classification of CII systems to on-site checks

- **Security by design** not only contributes to trust but makes the verification and thus certification of technologies easier

- Increasing trustworthiness level for solutions on a base of clear **trust architecture** specific to the regulation

- Combination of state-of-the-art solutions with services supporting the proper **security maturity level**
IoT VULNERABILITIES, THREATS AND RISKS
Kaspersky Lab ICS CERT identified 63 vulnerabilities in industrial and IIoT/IoT systems in 2017.
IoT VULNERABILITIES

Adversary
Weaknesses can be used for:

- BotNets
- Backdoors
- Privacy violation
- Data theft
- Spying
- Extracting private credentials

Cloud
- Week security policies, access control
- SSL vulnerabilities
- OWASP TOP10
- Shared responsibility

Insecure communications (week encryption, authentication, verification, etc)

Adversary Controls

Sensors

Gateway
- Vulnerabilities in firmware, software, physical interfaces
- Insecure web interface
- Open insecure ports
- Outdated protocols (e.g. SIP)
- Inherent vulnerabilities

Laptop

Mobile

Threat surface

APP

Server

Database

Mobile

Laptop

Cloud

Database
IOT ATTACK SCENARIOS

- MITC: Man in the Cloud
- User impersonation
- Plant backdoors
- Buffer overflow
- SQL Injection
- Privilege escalation
- Side channel
- DDoS
- Data integrity
- Certificate spoofing
- Phishing
- Drive-By-Download
- Brute Force
- Password reset

Remote attacker

Cloud

Server

Database

APP

Database

Gateway

Sensors

Controls

Has access to the local network

Has direct access to the device

Mobile

Laptop

Attack surface

• Intercepting communications
• Man In The Middle
• Device discovery via SSDP/UPNP
• Unauthorized access and app execution

• Device discovery through open ports
• Device vulnerabilities discovery and exploit
• Intercepting communications

• Physical tampering
• Infiltration during manufacturing
• Configuration change
• Malware
• Sim replacement
IOT SECURITY ELEMENTS

- DDOS protection
- Advanced persistent threat protection
- Various servers protection: Web, Mail, File...
- Virtual machines and hypervisors protection
- Secure Hypervisor
- Security Orchestration
- Perimeter protection

- Whitelisting: apps, communications, devices
- Antivirus
- Reputation assessment
- Vulnerabilities Detection
- Firewall

- Secure execution environment
- Security domain separation
- Strict policies: apps, communications, devices, users
- Vulnerability detection
- Patch management

- Communication anomalies and violations detection (DPI, Machine Learning)
- Intrusion detection
- Network filtering

- Secure OS
- Vulnerability detection
- Strict policies: apps, communications, devices, users
- Patch management
- State monitoring
BEST PRACTICES
IIC IoT SECURITY MATURITY MODEL
# IIC ENDPOINT SECURITY BEST PRACTICES

## Intentional violation using simple means and limited resources

**BASIC**
- Secure Communications
- Cryptography
- Endpoint Identity
- Secure Lifecycle
- Root of Trust

## Intentional violation using sophisticated means and sufficient resources

**ENCHANCED**
- Endpoint Configuration & Management
- Secure Communications
- Cryptography
- Endpoint Identity
- Secure Lifecycle
- Root of Trust

## Intentional violation using sophisticated means and large resources

**CRITICAL**
- Security Information & Event Management
- Endpoint Configuration & Management
- Secure Communications
- Cryptography
- Endpoint Identity
- Secure Lifecycle
- Root of Trust
- Policy & Activity Dashboard

---

IIC:WHT:IN17:V1.0:PB:20180312
MILS - MULTIPLE INDEPENDENT LEVELS OF SECURITY
PRACTICAL STEPS
THREATS

- MITIGATIONS
  - DYNAMIC RESPONSE
    - HCI
    - ICS CERT
  - PROACTIVE DEFENSE
    - KATA
    - KICS
  - TRUSTED INTEGRATION
    - Assessment
    - AAA
    - PKI
    - MDM

- PREVENTION
  - KSN/KPSN
  - Policy Control
    - Security Events
  - KL Agent
  - MNGMNT PL
  - CONTROL PL
  - MDM

- TRUST BASE
  - KSC/MDM
  - FIREWALL
  - DATA PLANE
  - Trusted Channel

GATEWAY

- ATTACK/ANOMALY DETECTION
  - ML Preproc
  - ML Engine
  - KATA Integr
  - Asset Detection
  - KICS/KATA

- SERVICE DEPLOYMENT
  - URL/DNS Filter
  - Antimalware
  - VPN
  - DPI
  - IPS/IDS
  - KL Agent

EDGE

- APPLICATION SECURITY
  - Whitelisting
  - Antimalware
  - Content Filt
  - Asset Detection
  - KES

- POLICY INFORCEMENT
  - Temporal Logic
    - Inter-process Communication
  - RBAC
    - Domain Isolation
  - KSS

- TRUSTED KERNEL
  - TEE
  - Trusted LC
  - KOS/KSH

TRUSTED COMMUNICATIONS

- MNGMNT PL
  - FIREWALL
  - CONTROL PL
  - DATA PLANE
TOOLS FOR SECURITY BY DESIGN

KASPERSKYOS
- Most secure solution (all components are isolated and controlled)
- Requires rethinking and redevelopment of architecture of every component
- Requires (at least) porting of applications or complete rewriting of them
- Limited support of hardware (embedded systems only)

SECURE HYPERVERSOR
- Good level of security (isolation of VMs and critical functions, limited control of communications)
- Requires rethinking and redevelopment of applications’ architecture only
- Requires re/development some critical functions
- Wide range of hardware supported (not only embedded systems)

KSS FOR LINUX
- Good level of security (isolations of Linux containers, control only inter containers communications)
- Requires rethinking and redeveloping of applications’ architecture only
- Requires minimum re/development
- Runs virtually on all Linux with containers support
IOT GATEWAY

Malware Delivery Thru Data Storage Device
Malicious Firmware Update
Exploiting Software Vulnerabilities
Attack on Key / Certificate Stores
Attack from Downloaded Apps
Man-in-the-Middle Attack

Internet Provider (ISP)
Server
Database
APP
Database

Smart camera
Smart light
Smart socket
Smartphone
Laptop
Smartphone

Sniffing of User Data
Attack from Mobile Device
Password dictionary attack
DDoS Attack
Exploiting Software Vulnerabilities
Malware
KASPERSKY SECURE IoT GATEWAY

**Secure Boot**
- Boots only verified firmware
  - Firmware is digitally signed and encrypted
  - Bootloader is verified
  - Only trusted OS is loaded

**Secure Update**
- Guarantee integrity and authenticity of the firmware delivery
  - Failsafe rollback
  - Firmware lifecycle support

**Secure Lifecycle Device Management**
- Security policies enforcement by independent engine
- Controls interactions across the system
- Security domains separation

**Secure OS**
- Kaspersky Security Network
- Threat Data Feeds
- Firmware Checking
- Vulnerability Assessment

**Security Services**
CONNECTED CAR – ATTACK VECTORS

- Malware through removable storage
- Downloaded software
- User data theft
- Man-in-the-Middle
- Using code vulnerabilities
- Malware through Firmware
- OBD2 attack
- Remote attack on the central bus
- Attacking actuators
- Attack on certificate storage
- Attack from the mobile device
- User data theft
<table>
<thead>
<tr>
<th>Threat vectors</th>
<th>KL Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Car Cloud Services</strong></td>
<td><strong>Server Security, Solutions for Data Centers, DDoS Protection, Security Assessment Services (SAS)</strong></td>
</tr>
<tr>
<td>• Man in-The-Middle-Attack</td>
<td></td>
</tr>
<tr>
<td>• Attack From Downloaded Apps</td>
<td></td>
</tr>
<tr>
<td><strong>Network Access</strong></td>
<td><strong>Security and Vulnerability Mgmt (SVM), IDS &amp; IPS, Mobile SDK, Security Assessment Services (SAS)</strong></td>
</tr>
<tr>
<td>• Sniffing of User Data</td>
<td></td>
</tr>
<tr>
<td>• Attack From Downloaded Apps</td>
<td></td>
</tr>
<tr>
<td>• Exploiting Software Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>Car Gateway</strong></td>
<td><strong>IPS technology can be transformed to IDS, Security and Vulnerability Mgmt, Anti-Malware, Security Asmmt. Services, Kaspersky Secure Hypervisor, Kaspersky Security System SDK (IPS), KasperskyOS</strong></td>
</tr>
<tr>
<td>• Attack from Apps in Mobile Device</td>
<td></td>
</tr>
<tr>
<td>• Exploiting SW Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>• Malicious Firmware Update</td>
<td></td>
</tr>
<tr>
<td>• Malware Delivery Thru Data Storage Devices</td>
<td></td>
</tr>
<tr>
<td><strong>Car Network</strong></td>
<td><strong>Security Assessment Services, Kaspersky Security System SDK (IPS)</strong></td>
</tr>
<tr>
<td>• Compromised Engine Actuator</td>
<td></td>
</tr>
<tr>
<td>• Attack on Vehicle Bus</td>
<td></td>
</tr>
<tr>
<td><strong>ECU</strong></td>
<td><strong>Kaspersky Security System SDK (IPS), Encryption, Security Hypervisor, Security Assessment Services, KasperskyOS</strong></td>
</tr>
<tr>
<td>• Attack on Key,</td>
<td></td>
</tr>
<tr>
<td>• Malicious Firmware Update</td>
<td></td>
</tr>
<tr>
<td>• Attack on Vehicle Bus</td>
<td></td>
</tr>
</tbody>
</table>
IN CONCLUSION
TAKEAWAYS

• Market: Critical Information Infrastructure
• Regulation: National Landscape
• International Cooperation: ITU, IIC, GSMA, GP
• Principle: Security by Design
• Foundation: Integrated Security
LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com