Protecting Corporate Data from Mobile Threats…

And the emerging role for microSD-based security

Art Swift
CEO, CUPP Computing
Information security is broken

$77B
WORLDWIDE SPENDING ON INFORMATION SECURITY IN 2015

$400M
FINANCIAL LOSS FROM 700 MILLION COMPROMISED RECORDS

99.9%
VULNERABILITIES EXPLOITED MORE THAN A YEAR AFTER CVE WAS PUBLISHED

70-90%
OF MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION

23%
OF INCIDENTS INVOLVE STOLEN CREDENTIALS

95%
OF INCIDENTS INVOLVE STOLEN CREDENTIALS

How Data Breaches Occur

$400M
FINANCIAL LOSS FROM 700 MILLION COMPROMISED RECORDS

$77B
WORLDWIDE SPENDING ON INFORMATION SECURITY IN 2015

99.9%
VULNERABILITIES EXPLOITED MORE THAN A YEAR AFTER CVE WAS PUBLISHED

70-90%
OF MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION

23%
OF INCIDENTS INVOLVE STOLEN CREDENTIALS

95%
OF INCIDENTS INVOLVE STOLEN CREDENTIALS

Average financial losses due to security incidents:

2013
$0.65 million

2014
$0.41 million

2013
$1.0 million

2014
$1.3 million

2013
$3.9 million

2014
$5.9 million

Small
Revenues less than $100 million

Medium
Revenues $100 million-$1 billion

Large
Revenues more than $1 billion

And the data breach pandemic continues

Mobile attack vectors threaten corporate data

Mobile security threats

- Unpatched OS and apps
- Malware on appstores
- Malicious payloads / attachments
- Drive by attacks (browser)
- Unsecured public Wi-Fi
- Rogue cell tower (stingray)
- Jailbreaking / rooting
- Auto-download of malicious MMS

Corporations are demanding solutions

In a recent international survey of IT decision makers*…

93%
Believe mitigating targeted attacks is a high, urgent or critical priority

91%
See preventing data breach by mobile as high, urgent or critical

90%
Rate regulatory compliance as high, urgent or critical issue

74%
Demand stronger hardware based security!

And microSD-based security appliances can address this need, particularly for Android smartphones and tablets…

* Source: Decisive Analytics LLC, Multinational Security Decision Makers Study 2015 – Commissioned by CUPP Computing
CUPP creates a hardened shell around the device

How the security engine works

- Intercepts all network traffic
- Scans each packet for exploits
- Scans each payload for malware
- Filters unwanted apps / appstores
- Blocks low-reputation websites
- Blocks access to known CCS
- Alerts admin of intrusion attempts

CUPP vs. security software approach

Self-contained hw subsystem
- Completely isolated from host OS
- CPU optimized for security tasks
- Hardened open source kernel
- Onboard low-power crypto engine
- Optimized high-speed SD bus
- Built-in IPS/IDS (firewall + snort)
- Encrypted memory up to 32GB
- Immune from mobile OS exploits
- Immune from mobile apps attacks
- Immune from rooting / jailbreaking
- Portable across user’s devices

Unique patented chip design
- MPU Atmel uProcessor
  ATSAM5D36A die - 4.6 x 4.1 mm
- LPDDR2 512MB RAM Micron
  U80M die - 8.5 x 9.5 mm
- NAND Flash Micron L83A Die x2 - 9.1 x 8 mm (stack)
- NAND Flash driver Hyperstone S8
  Die - 1.8 x 3.8 mm
- Lattice FPGA LCMX02-4000 ZE
  Die - 3.8 x 3.7 mm
- Total of 40 R L C
### MicroSD-based security market forces

#### Demand Side
- Data breach is a pandemic
- Strong demand for solutions
- Tough regulatory environment
- Increased BYOD usage
- Consumerization of IT
- Widespread Android deployment
- Increased use of Android tablets

#### Supply Side
- Moore’s law
  - High performance CPUs
  - Memory die size shrinks
  - Low power FPGA
- Advances in packaging
- Security paradigm advancements
- MDM, MAM commoditization
- Funding availability for Hardware
Take-aways

✓ Traditional IT security is broken
✓ Data breach pandemic continues
✓ CSO’s are demanding HW solutions
✓ MicroSD form factor can help
✓ CUPP has built the world’s first microSD-based security appliance!