Embedding IoT Chip Security Using eBeam Solutions

David K. Lam

Multibeam Corporation

Member of eBeam Initiative

San Jose, CA – September 12, 2016

Are Cyberattacks Real Dangers?

Bloomberg June 10, 2015

Hackers' Favorite Target:
Big Oil and All That Deadly Equipment

FINANCIAL TIMES Jan. 6, 2016

Hackers shut down
Ukraine power grid

THE WALL STREET JOURNAL. May 20, 2016

Swift Banking Network Struggles
With Wave of Cyberattacks

Healthcare IT News April 4, 2016

Two more hospitals
struck by ransomware

What's IoT Got to Do with It?

“CyberWar Threat”*

“Imagine a world with 50 Billion microprocessors attached to the internet, that’s 50 Billion points of attack”

“Instead of bullets and bombs, you use bits and bytes”

“All you would need to do is take out about 9 substations, in an attack that could result in a blackout for the majority of the U.S. that could last for weeks or months”

*Excerpts from “CyberWar Threat,” Aired October 14, 2015 on PBS NOVA.
http://www.pbs.org/wgbh/nova/military/cyberwar-threat.html

MULTIBEAM

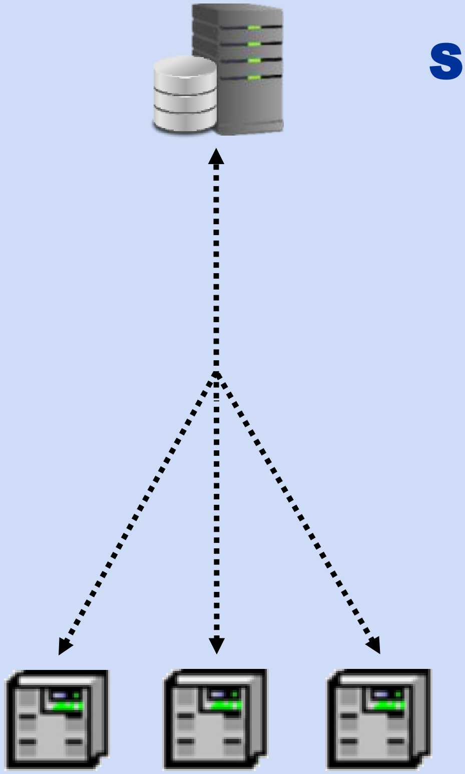
What’s in an IoT Device?

- Simple microcontroller; limited resources, memory
- Sensor/actuator, Internet connection
- Doing simple tasks

What’s Not in an IoT Device?

- No defense against hacking

Industrial Control System (ICS)



SCADA

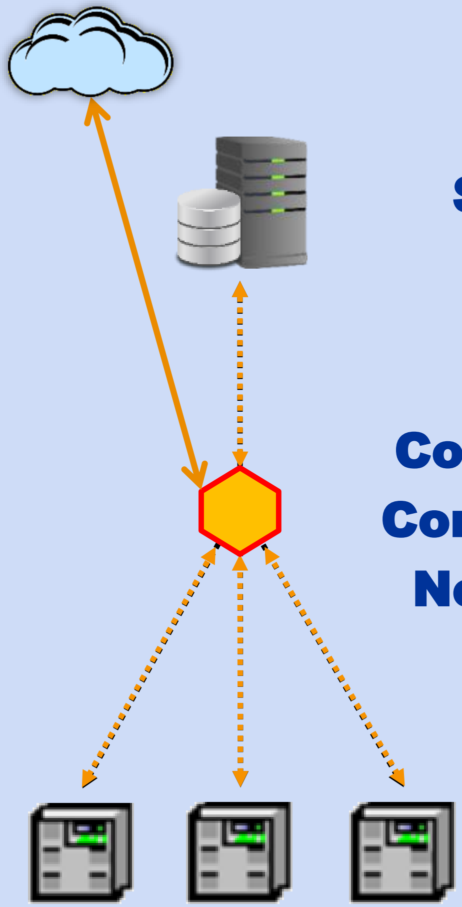
- Remotely control/monitor critical infrastructure
- Collect & analyze real-time data; adjust PLC
- <u>No network security</u>

Obscurity is Security

PLC

- PLC = microcontroller + sensor/actuator + comm.
- Doing simple tasks in electromechanical systems
- <u>No defense against hacking</u>

Industrial Control System (ICS)



SCADA

- Remotely control/monitor critical infrastructure
- Collect & analyze real-time data; adjust PLC
- <u>No network security</u>

Company Computer Network

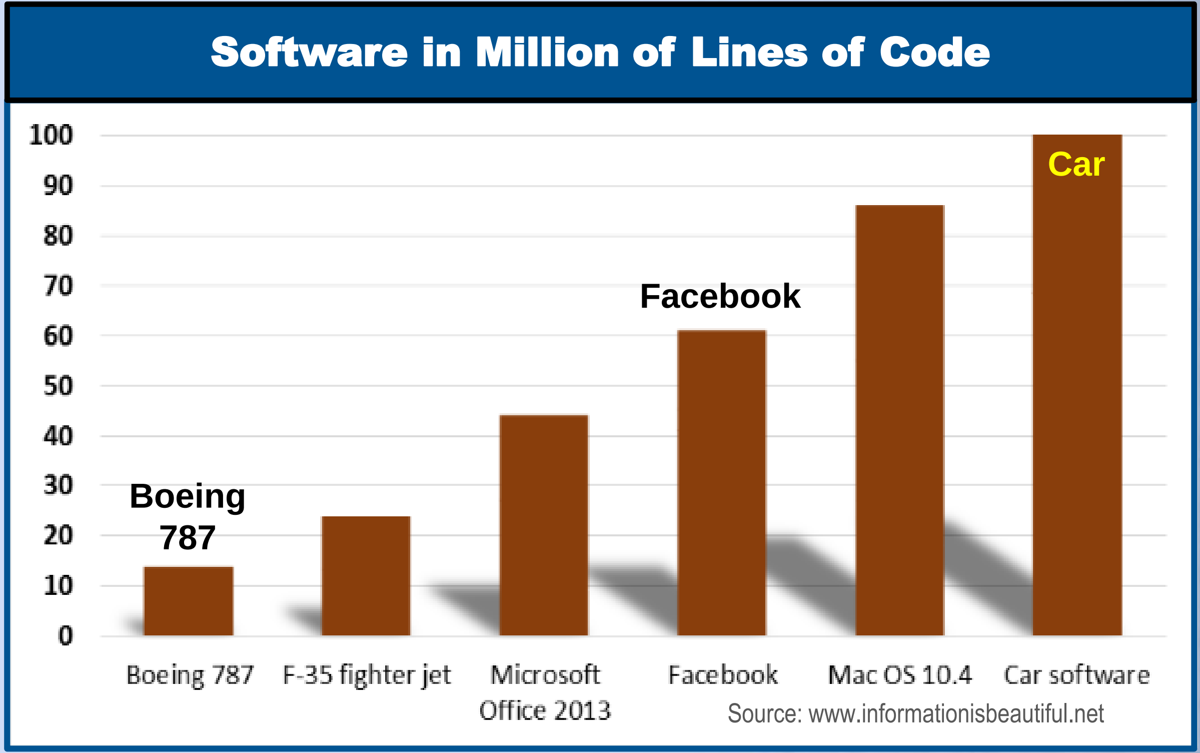
- SCADA patched into company computer network
- SCADA internet-accessible – <u>not intended originally</u>
- <u>Infrastructure vulnerable to hacking</u>

PLC

- PLC = microcontroller + sensor/actuator + comm.
- Doing simple tasks in electromechanical systems
- <u>No defense against hacking</u>

Connected Cars Have Arrived

Can Software Alone Assure Auto Security?



Source: www.informationisbeautiful.net

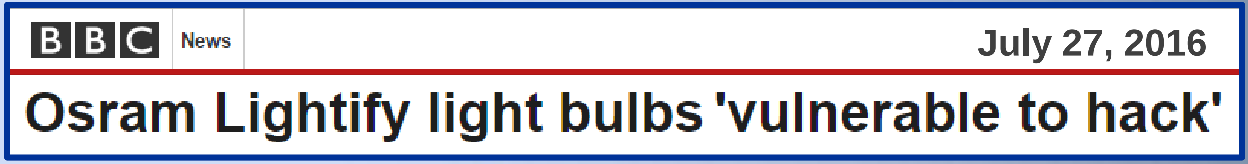
“Motor vehicles increasingly vulnerable to remote exploits.”

– FBI warning, *March 17, 2016*

- Hackers exploit defects to breach software defenses
- “Defect-free software does not exist.”

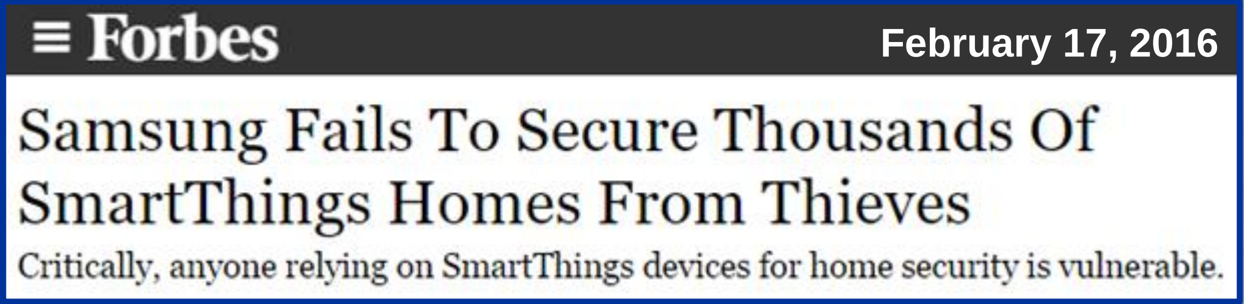
– Wietse Venema, *Google*

Are Connected Homes Secure?



BBC News July 27, 2016

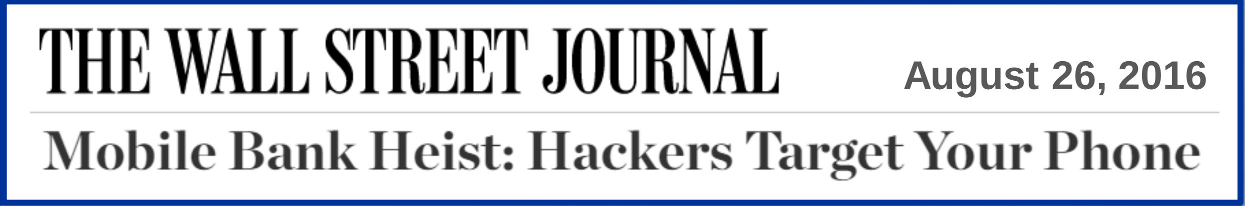
Osram Lightify light bulbs 'vulnerable to hack'



Forbes February 17, 2016

Samsung Fails To Secure Thousands Of SmartThings Homes From Thieves

Critically, anyone relying on SmartThings devices for home security is vulnerable.



THE WALL STREET JOURNAL August 26, 2016

Mobile Bank Heist: Hackers Target Your Phone

Connectivity Is Vulnerability?

- **50 billion connected devices enlarge attack surface**
- **“A successful breach of one subsystem becomes the staging point for attacks on other subsystems.”**

– Mike Borza, *CTO Security, Synopsys*

IoT Devices Need
Both Hardware & Software Security

- IoTs need software updates to patch vulnerabilities
- IoTs need hardware security to authenticate software
- IC-embedded security is foundation of a secure system

On-Chip Hardware Solutions Today

Fuse programmable IC	• Security info fused at outermost layer at device test • Data may be exposed to 3rd party and compromised • Fused data not embedded, could be accessed/changed
"Non-volatile" memory	• Security info programmed in Flash after IC is made • Flash designed to be accessible, updatable in the field • Retention 5-10 years, much less than infrastructure life

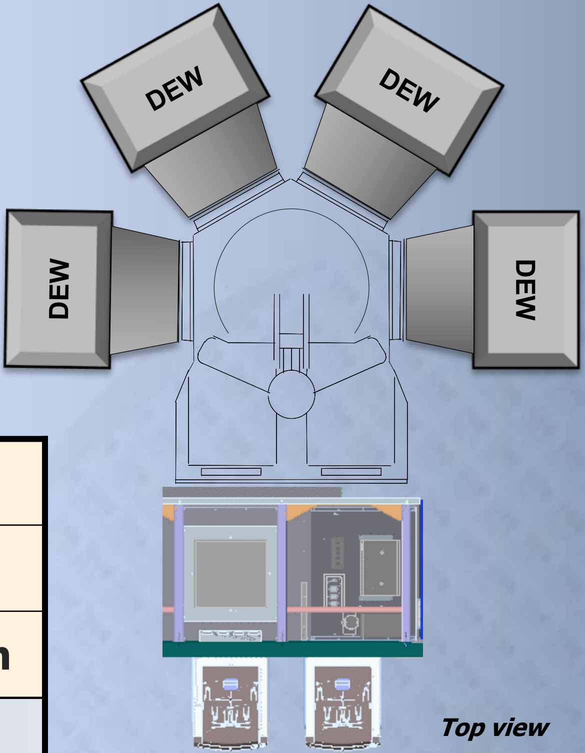
Direct Electron Writing (DEW)

Personalizing ICs with Unique Info

- Chip ID, MAC address
- Private key encryption
- Other security info / features

Security Data

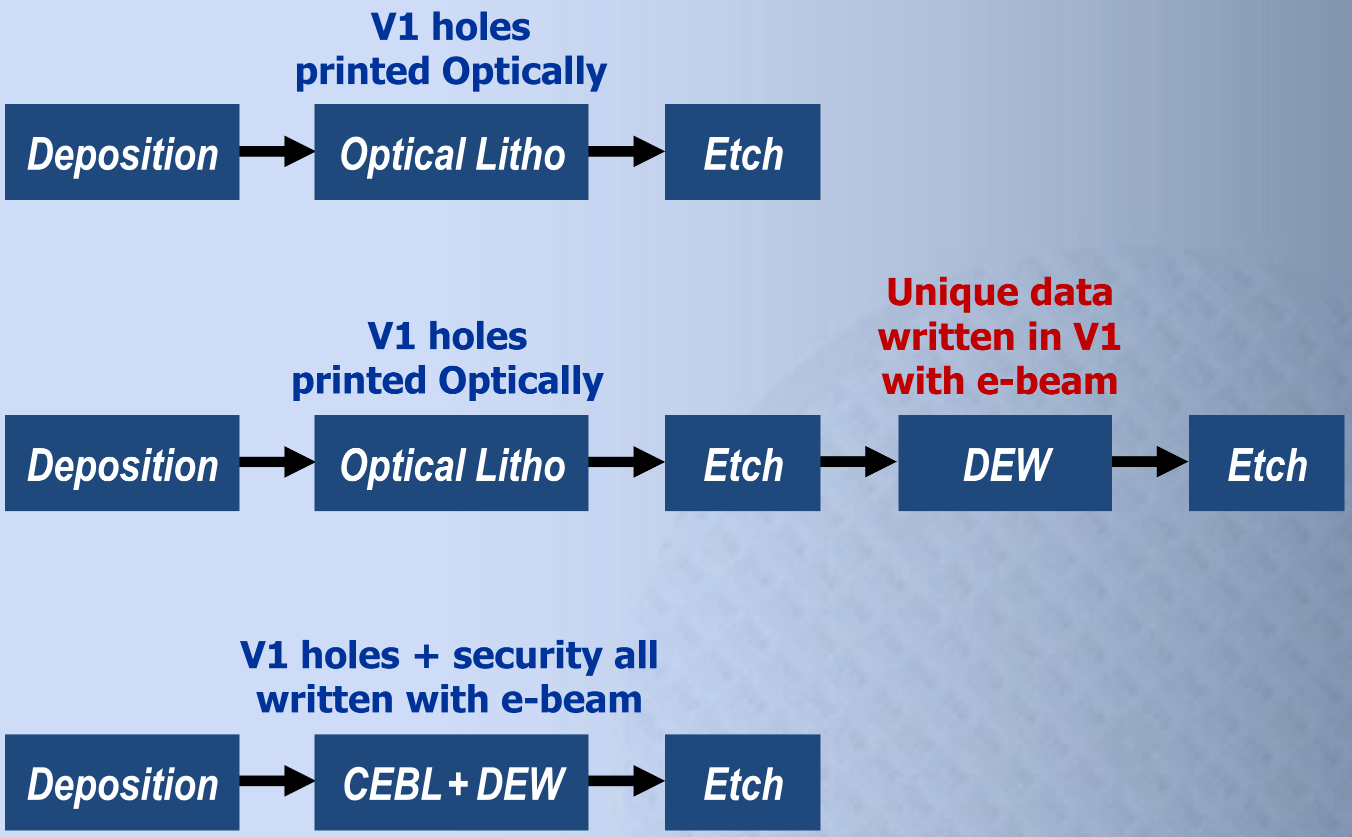
MAC address	ID for Internet communication
Chip ID	Anti-counterfeit, anti-tamper
Private key	Secure software authentication
IDs readable but not alterable	
Private key not accessible from outside IC	



DEW Writer

What DEW Does In Wafer Fab

Example: Via-1 Layer Simplified



Regular production flow with no Security

V1 holes printed Optically

Deposition → Optical Litho → Etch

Security info embedded in V1 using DEW

V1 holes printed Optically

Unique data written in V1 with e-beam

Deposition → Optical Litho → Etch → DEW → Etch

E-beam writes Vias & Security in V1 layer

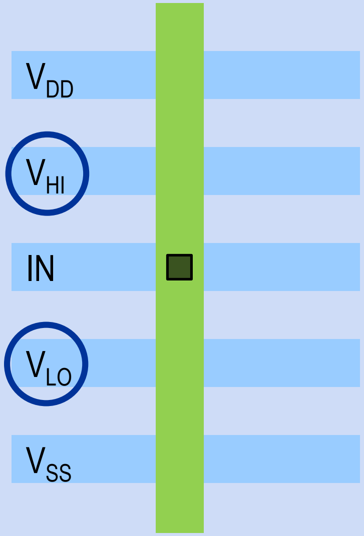
V1 holes + security all written with e-beam

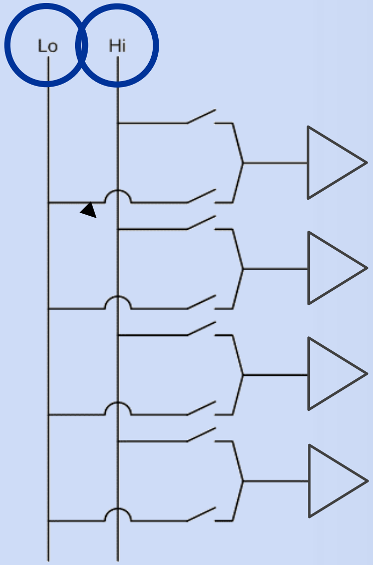
Deposition → CEBL + DEW → Etch

How DEW Embeds Security

Example: Embedding Encryption Key

- IC design includes "Hi" & "Lo" signals and "In" to a gate

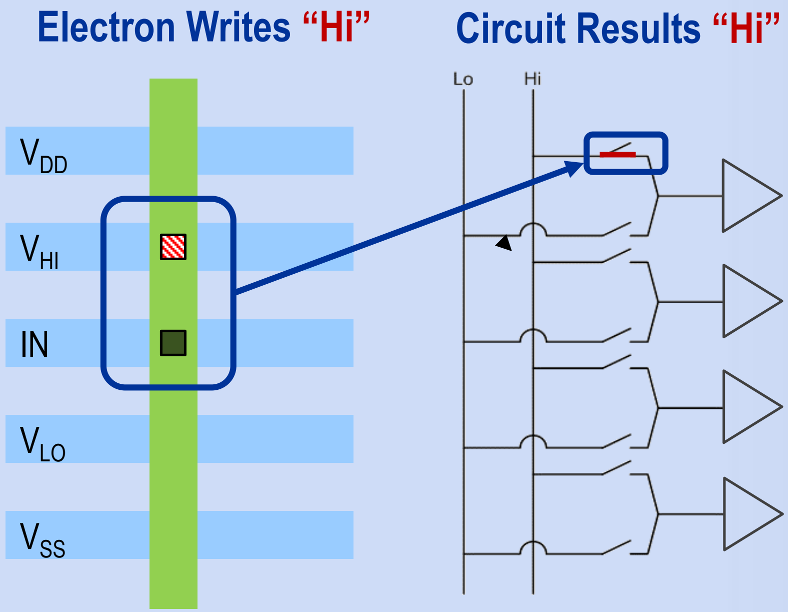




How DEW Embeds Security

Example: Embedding Encryption Key

- IC design includes “Hi” & “Lo” signals and “In” to a gate
- DEW writes hole in “Hi”, circuit results in “Hi”.



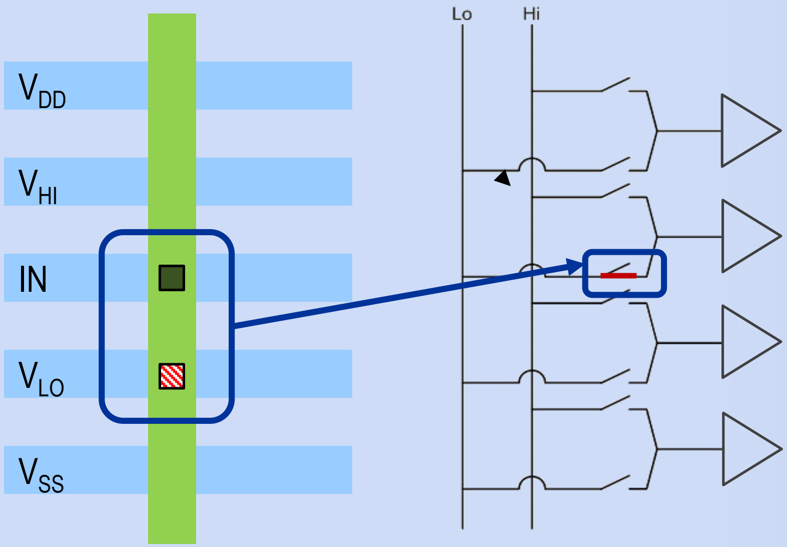
Electron Writes “Hi”

Circuit Results “Hi”

How DEW Embeds Security

Example: Embedding Encryption Key

- IC design includes “Hi” & “Lo” signals and “In” to a gate
- DEW writes hole in “Hi”, circuit results in “Hi”. Likewise for “Lo”

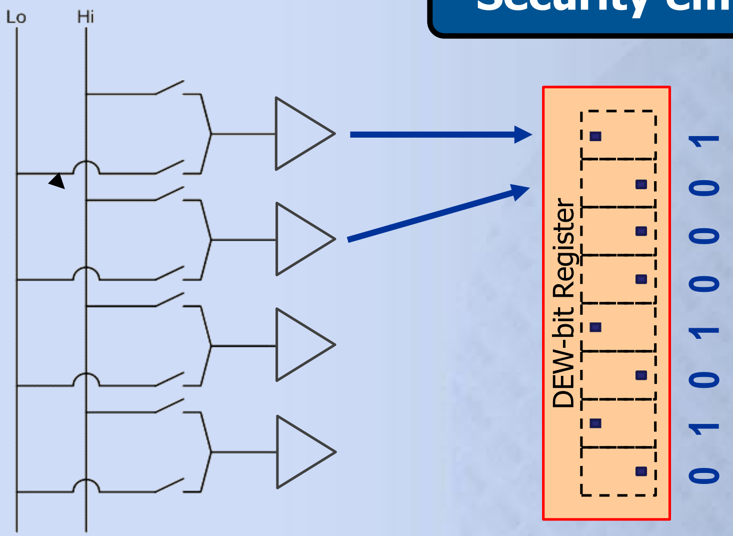


Electron Writes “Lo” Circuit Results “Lo”

How DEW Embeds Security

Example: Embedding Encryption Key

- IC design includes “Hi” & “Lo” signals and “In” to a gate
- DEW writes hole in “Hi”, circuit results in “Hi”. Likewise for “Lo”
- After wafer is processed, encryption key is embedded



Security embedded in IC

Q: Can the Connected World be more secure?

A: Yes, but we need a new approach.

- Security is designed in, not an afterthought
- Security is written into every IoT chip such as with DEW
- Chip-embedded security complements software security to bolster cyber-defense