



Hacking AMI



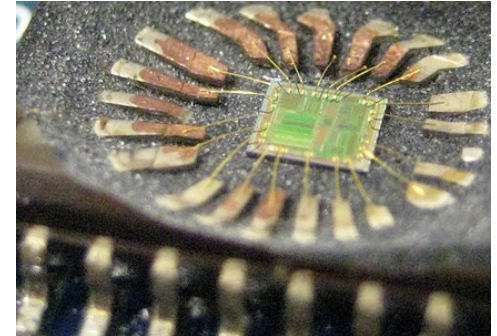
Problems in AMI

- Embedded systems have received limited attention from the security community
 - Little is known about hacking them (publicly)
 - AMI systems have received even less attention
 - Wild Wild West!
- Implications to Improperly Secured Non-Embedded Systems are **Huge**
 - Change the face of the western world...



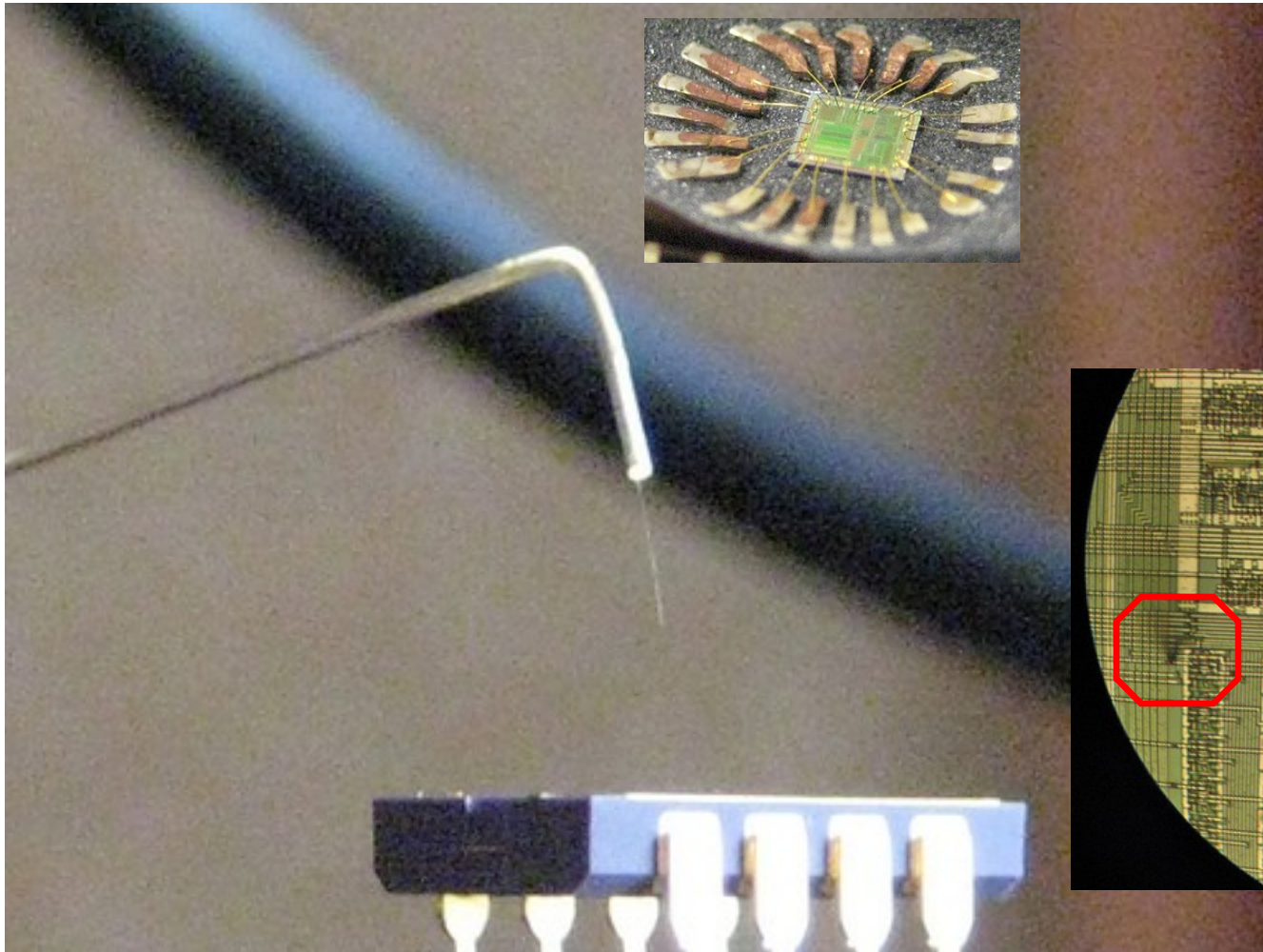
AMI Embedded Systems

- Insecure data busses and serial connections
 - C12.22 bus
 - Data Capture, Injection (both directions)
 - Radios
 - MCU's
- Stealing/Replacing Keys In Memory
 - Network Encryption
 - Authentication and CA keys
- Blown JTAG Fuse Isn't Enough
 - Third-party labs remove top/allow microscopic access to chip
- Firmware-level vulnerabilities similar to x86 systems
- **It's the Latch!**

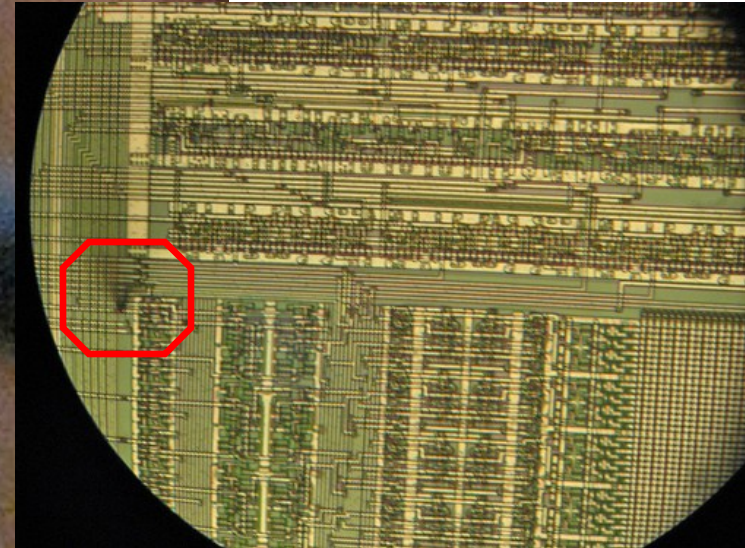




Microscopic Probe



- Decapitated Chip
- Microtuned Placement
 - Access Memory
 - Reset the JTAG fuse





AMI-SEC and ASAP

- AMI-SEC Taskforce
 - ASAP (AMI-SEC Acceleration Project)
 - Red Team Testing (hacking)
 - Darren Highfill <darren@enernex.com>
 - <http://osgug.ucaiug.org/utilisec/amisec/>

- Matthew Carpenter
 - InGuardians
 - ASAP Red Team Lead
 - matt@inguardians.com

Core ASAP Attack Team



- The ASAP Attack Team:
 - Travis Goodspeed
 - Josh Wright
 - Matthew Carpenter

