

Access Control Class

You've worked hard to secure your servers, workstations, and network. But increasingly, your physical security is tied into electronic access control systems, bringing major exposure to your enterprise if these systems aren't secured properly. How can you trust your systems if their physical security is in jeopardy? Every security pro should have some skills in assessing access control systems, and this class provides exactly what you need.

Whether an enterprise is using HID Prox cards, NXP Hitag chips, Mifare credentials, or even iCLASS technology, students who have taken this course will be well-versed in the functionality, weaknesses, and attack vectors of such systems. From how to perform practical card cloning attacks in the field to advanced format downgrade attacks, students are prepared for real-world red team scenarios and learn how to exploit access control technology with the latest attack hardware.

Outline:

- Access Control History and Design Elements
- 125KHz Credentials:
 - AWID, Overview and Cloning
 - EM4102/EM4200, Overview and Cloning
 - HID Prox / ProxCard II, Overview and Cloning
 - Kantech ioProx / ioProx XSF, Overview and Cloning
 - Atmel T5555 / T5577 Tags, Emulation Overview and Cloning Capabilities
 - Motorola / HID Indala Overview, and Cloning
 - Overview of other uncommon credentials
- 125/134KHz Vehicle Transponders:
 - NXP Hitag (PCF7931) Overview, and Cloning
 - NXP Hitag II (PCF7936) Overview, and Cloning
- 13.56MHz Credentials and Smart Cards:
 - HID iCLASS Deep Analysis, Review, Reverse Engineering, Cloning, and Weaknesses
- Advanced Attacks and Configuration Cards
 - NXP Mifare Classic Detailed Overview, Cracking, Cloning, Weaknesses
- Overview of other common and uncommon credentials, with discussion of security implications and strengths of each
- Practical Cloning in the Field, Advanced Format Downgrade Attacks
- Backend Detailed Overview, Weaknesses, and Attacks:
 - Man in the Middle
 - Denial of Service
 - Defeating Tamper Detection
 - Defenses and Mitigation
- Electronic Access Control Attack Tools