



PANEL #1

Theme: Challenges and Costs on Robust and Cyber-protected Systems

Moderator: Prof. Dr. Erik Buchmann, ScaDS.AI Dresden/Leipzig, Germany

Panelists:

Prof. Dr. Alexander Lawall, IU International University of Applied Sciences, Germany

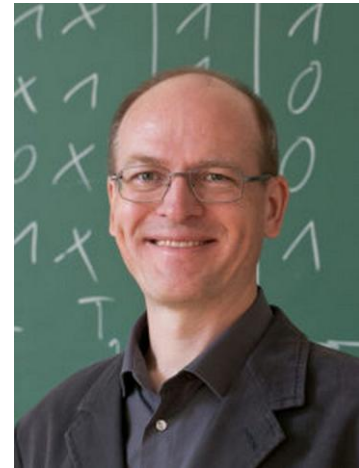
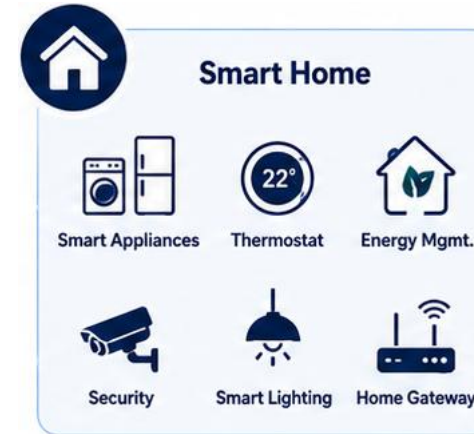
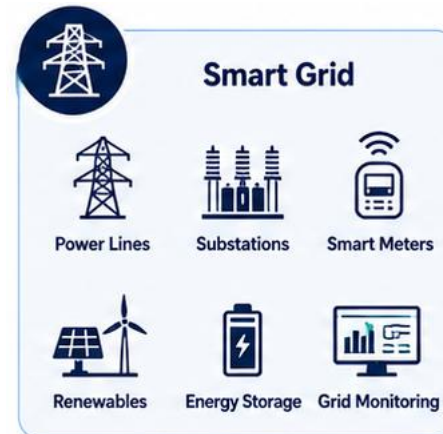
Viktoriia Vovchenko, Bielefeld University of Applied Sciences and Arts, Germany

Prof. Dr techn. Jörn-Marc Schmidt, IU International University of Applied Science, Germany



Today's Systems are Smart

- On multiple layers:
 - mission
 - system architecture
 - software/data
 - supply chain
 - users/operations

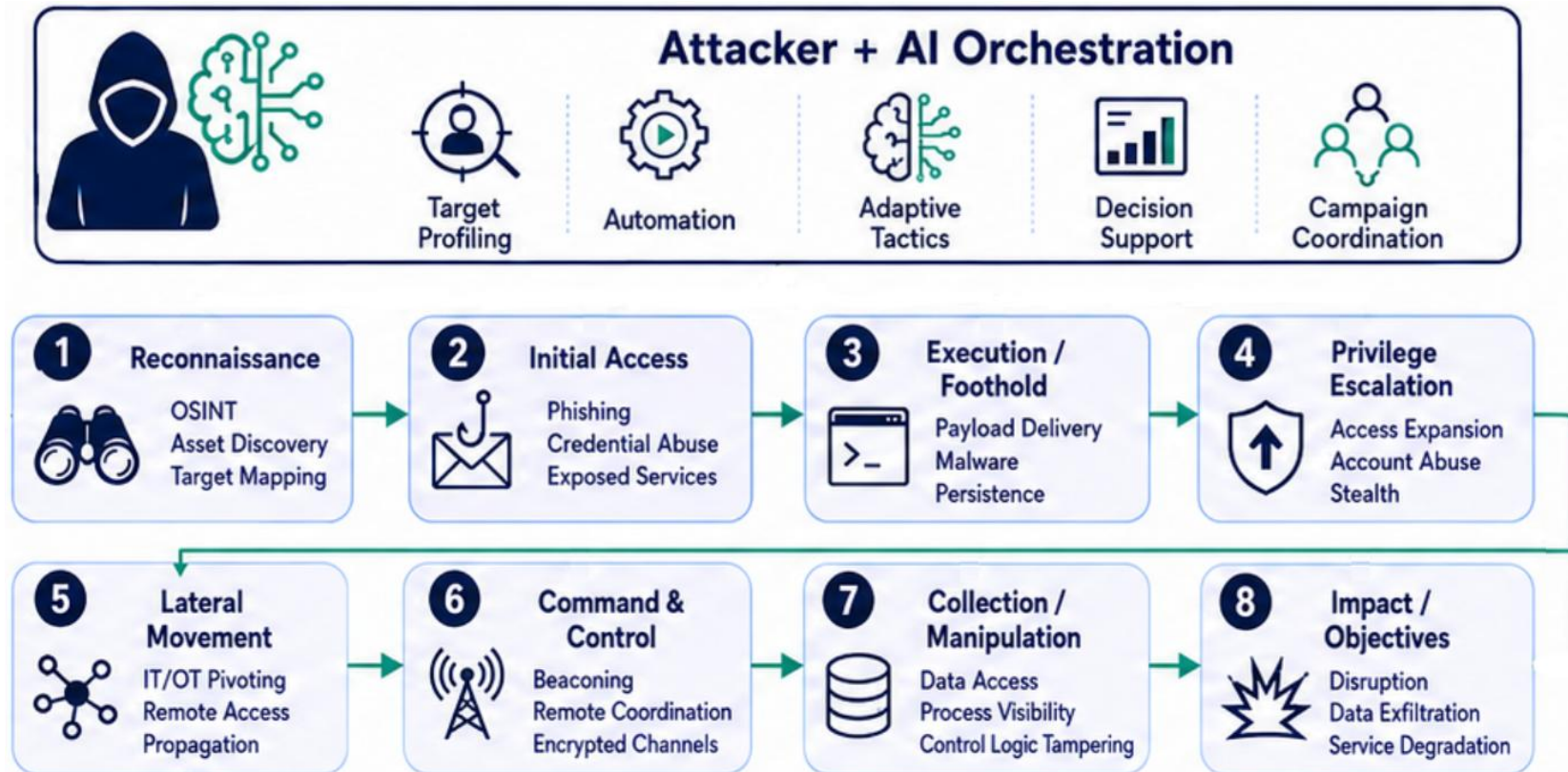


Erik Buchmann
*Center for Scalable
Data Analytics and
Artificial Intelligence
Dresden/Leipzig,
Germany*



Today's Attackers are also Smart

- The hard part is not *one* threat, but the interaction of *many* threats:
 - complexity
 - legacy systems
 - AI agents
 - dependencies
 - regulation
 - human operations
 - ...





Challenges and Costs on Robust, Cyber-protected Systems?

- *Challenges*

- Larger attack surfaces: cloud, IoT, APIs, remote access
- Supply-chain and third-party risk
- Safety/security trade-offs in critical systems
- Verification limits: cannot test every attack path
- Governance gap: who owns residual risks?

- *Costs*

- Engineering cost: secure design, testing, redundancy
- Operational cost: monitoring, patching, incident response
- Compliance cost: documentation, audits, certification
- Failure cost: downtime, breach response, liability, reputation



(Possible) Discussion Areas

- **How much cybersecurity can a system realistically afford?**
 - At what point do security investments exceed their economic benefit?
 - How can the ROI of cybersecurity be measured?
 - Is “maximum security” technically or economically achievable?
 - Comparing the cost of prevention vs. the cost of recovery after incidents.
- **Can AI secure systems faster than AI can attack them?**
 - AI-driven intrusion detection & Autonomous cyber defense
 - Adversarial machine learning & Prompt injection attacks
 - Manipulation of AI models
- **Should we accept that systems will eventually be compromised?**
 - Prevention → resilience
 - Recovery-first strategies
 - Self-healing systems



Alexander Lawall

IU International
University of
Applied Sciences

▪ Easy access to AI brings additional security risks

- Security risks stemming from generative AI excellence;
- Deepfakes have never been easier or cheaper to create;
- No (little) expertise is needed to use AI;
- The catch-up game of AI-detection: AI classifiers fall behind.



Viktoriia Vovchenko
Bielefeld University of
Applied Sciences and Arts



■ **Securing the System-in-Context**

- Security must include the System's Operating Environment, not just the System itself
- Cybersecurity and Safety become inseparable in Cyber-Physical Systems
- More Connectivity increases Capability but also expands the Attack Surface



Jörn-Marc Schmidt
IU International
University of Applied
Science,
Germany

The question is not only, **“Can the system be hacked?”** but also, **“Can the world around the system — intentionally or unintentionally — cause unsafe behavior?”**



STAGE IS YOURS!