Collaboration Notes: Dr. Olga Gadyatskaya

Associate Professor - Cyber Security

Background Research

Key Projects & Initiatives

1. **C-SIDe Project (€1.45M, 2021-2025)**
   - Cyber-Security-by-Integrated-Design
   - Lead LIACS researcher for interdisciplinary security approach
   - Partners: ISGA, Hague University, NCSC, SURF, LUMC
   - Focus: Integrating security throughout software development lifecycle
2. **Leiden Organizational Cyber Security (LOCS) Group**
   - Founded and leads this research group
   - Focus on organizational security, not just technical
   - Website: https://locs.liacs.nl/
3. **Recent Research Focus**
   - Explainable AI for Android malware detection
   - Security in federated learning
   - GitHub exploit code analysis (found malicious codes targeting pen testers)
   - Secure software development methodologies

PhD Students (Current)

- Arina Kudriavtseva: Secure software engineering programs (C-SIDe)
- Jafar Akhoundali: Secure software for large-scale systems (C-SIDe)
- Rui Li: Explainable malware detection (CSC scholar)
- Xinyuan Ji: Security/privacy in federated learning

Understanding Security-by-Design

Traditional vs. C-SIDe Approach

Traditional Security-by-Design:

- Focus on technical steps only
- Involves only developers and security experts
- Often applied as afterthought
- Limited stakeholder engagement

C-SIDe Innovation:

- Holistic approach including human factors
- Involves psychologists, privacy experts, governance specialists
- Security integrated from conception
- Multi-stakeholder methodology

Key Concepts for Discussion

1. **Threat Modeling**: Systematic analysis of potential attacks
2. **Security Risk Management**: Organizational approach to security
3. **DevSecOps**: Integrating security into DevOps practices
4. **Explainable AI (XAI)**: Making AI decisions interpretable

Concrete Collaboration Ideas

Project 1: Secure API Education Platform

Goal: Develop educational framework combining jGuard with C-SIDe methodology

Technical Approach:

1. **Interactive Learning Environment**:
   - jGuard provides immediate runtime feedback
   - Explain WHY an API usage is insecure
   - Progressive difficulty levels
2. **Integration with C-SIDe**:
   - Apply multi-stakeholder approach to API education
   - Include psychological aspects of learning security
   - Measure effectiveness across different developer profiles
3. **Deliverables**:
   - Web-based platform for secure API training
   - Evaluation framework measuring learning outcomes
   - Best practices guide for security education

Why This Matters:

- Addresses the human factor in API misuse
- Scalable solution for industry training
- Direct impact through C-SIDe consortium

Project 2: Explainable API Misuse Detection

Goal: Apply XAI techniques to make jGuard's decisions understandable

Technical Approach:

1. **XAI Integration**:
   - When jGuard detects misuse, explain WHY
   - Generate natural language explanations
   - Adapt explanation complexity to developer expertise
2. **Machine Learning Component**:
   - Learn from developer interactions
   - Identify common misunderstanding patterns
   - Predict likely misuses based on developer profile
3. **Evaluation**:
   - User studies with different expertise levels
   - Measure comprehension and behavior change
   - Compare with traditional error messages

Connection to Her Work:

- Builds on her XAI for malware detection
- Applies her organizational security perspective
- Fits C-SIDe's interdisciplinary approach

Project 3: Mobile API Security Framework

Goal: Extend jGuard to Android development with C-SIDe principles

Technical Approach:

1. **Android-Specific Challenges**:
   - Permission system misuse
   - Inter-component communication vulnerabilities
   - Crypto API misuse on mobile
2. **jGuard for Android**:
   - Annotate Android APIs with guards
   - Runtime monitoring on mobile devices
   - Integration with Android Studio
3. **C-SIDe Methodology**:

- Study how mobile developers differ from others
- Consider user privacy expectations
- Policy recommendations for app stores

Benefits:

- Addresses her mobile security expertise
- Huge practical impact (billions of Android devices)
- Publication opportunities in top security venues

How to Present Your Ideas

Opening:

"I've been following your C-SIDe project and see strong synergies with my jGuard framework. Both aim to make security an integral part of development rather than an afterthought..."

Key Points to Emphasize:

1. **Interdisciplinary Nature**: Show you understand security isn't just technical
2. **Educational Impact**: jGuard as a teaching tool aligns with her interests
3. **Practical Applications**: Real-world impact through industry connections
4. **Human Factors**: Acknowledge the importance of developer psychology

Technical Terms to Use:

- **"Security-by-Design"**: Use consistently with her definition
- **"Multi-stakeholder approach"**: Key C-SIDe concept
- **"Organizational security"**: Not just technical solutions
- **"Explainable security"**: Making security decisions understandable

Questions to Ask Her

1. "How do you see the role of runtime enforcement in the C-SIDe methodology?"
2. "What are the main challenges in getting developers to adopt security-by-design?"
3. "How can we measure the effectiveness of security education interventions?"
4. "What's the relationship between explainable AI and developer trust in security tools?"

Potential Joint Activities

Papers:

1. **"jGuard: Runtime Enforcement for Security-by-Design"**

- Venue: USENIX Security or IEEE S&P
- Focus: Technical contribution with C-SIDe evaluation

2. **"Teaching Secure API Usage Through Interactive Runtime Feedback"**
   - Venue: SOUPS (Symposium on Usable Privacy and Security)
   - Focus: Human factors in security education
3. **"Explainable API Misuse Detection for Diverse Developer Populations"**
   - Venue: CHI or ICSE
   - Focus: Adaptive explanations based on expertise

Grants:

- **EU Horizon Europe**: Cybersecurity call (she has experience)
- **NWO Cybersecurity**: Follow-up to C-SIDe
- **Industry collaboration**: Through C-SIDe partners

Educational Initiatives:

- Co-develop security course modules
- Supervise joint MSc projects
- Industry workshops through C-SIDe

Understanding Her Network

Key Collaborators:

- **ISGA (Institute of Security and Global Affairs)**: Policy connections
- **NCSC (National Cyber Security Centre)**: Government relations
- **Hague University**: Applied research focus
- **SURF**: Research infrastructure
- **NeLL (National e-Health Living Lab)**: Healthcare applications

Industry Connections:

- Through C-SIDe consortium
- ONE Conference (European cybersecurity event)
- Pen testing companies (from her exploit research)

Cultural Fit

Her Values:

1. **Diversity**: Active in promoting women in cybersecurity

2. **Practical Impact**: Not just papers, but real-world change
3. **Interdisciplinary**: Embraces non-technical aspects
4. **Education**: Passionate about teaching and mentoring

How to Align:

- Mention interest in diverse teams
- Emphasize real-world applications
- Show openness to non-CS perspectives
- Express teaching enthusiasm

Preparation Tips

Before Meeting:

1. Read her GitHub malware paper (big impact)
2. Understand C-SIDe project structure
3. Prepare demo of jGuard with security education angle
4. Think about how jGuard fits organizational security

During Meeting:

- Be enthusiastic about interdisciplinary work
- Show you understand security is more than code
- Demonstrate how jGuard could help C-SIDe goals
- Ask about her vision for LOCS group growth

Key Differentiator:

Your jGuard provides the **technical enforcement mechanism** that C-SIDe needs to ensure their methodology actually gets implemented in practice.

References for Deep Dive

1. C-SIDe project website: projectcside.nl
2. Her GitHub malware findings (widely publicized)
3. SOUPS conference proceedings (usable security)
4. "The Programmer's Brain" by Felienne Hermans (understand her network)

Final Strategic Points

- She's building a group - opportunity to be founding member

- Recently promoted to Associate Professor - ambitious growth plans
- Strong funding track record - good for your career
- Bridges technical and human aspects - unique position
- Access to government and industry through C-SIDe