How to turn your KVM into a raging Key-Logging Monster חלק ב' - בשורות רעות

מאת ליאור אופנהיים ויניב בלמס

הקדמה

שלום חברים וברוכים השבים לחלק השני בסדרת המאמרים שלנו, בה ננסה להפוך KVM שולחני נחמד ותמים למפלצת Key-Logging זועמת.

החלק הראשון הסתיים בכך שהצלחנו לקבל 64K של מידע בינארי בלתי קריא לחלוטין מתהליך עידכון הקושחה של ה-KVM. במהלך העידכון המידע הבינארי הזה מועבר דרך הכבל הסיריאלי ועושה את דרכו דרך סבך המעגלים האלקטרוניים עד שמגיע בסוף דרכו אל מעבד ה-Winbond 8052 כאסמבלי 8051 תיקני.

או שזה לפחות הניחוש הטוב ביותר שלנו כרגע...

הבעיה עם ניחוש כזה, איך לומר את זה בעדינות, היא די קשה... למרות שזה נשמע לנו הגיוני לגמרי, ולמרות שראינו הרבה סימנים לכך שזה באמת המצב, עדיין יש סיכוי לא רע שאנו טועים.

הבעיה כאן היא שאם אנחנו רוצים לנסות ולפענח את שיטת הקידוד של המידע הבינארי, חשוב מאוד להבין איך צריכה להיראות התוצאה הסופית.

במידה וההנחה שלנו נכונה, התוצאה הסופית תיהיה אסמבלי 8051, אבל אם אנחנו טועים זה יכול להפוך את תהליך הפיענוח לסיוט מתמשך. אפשר אולי להשוות את זה לגרסה של משחק פוקר מבולבל, מוזר, בחדר חשוך לחלוטין עם קלפים ריקים על סכומים אינסופיים, עם מחלק שלא אומר לך את החוקים ומחייך כל הזמן[1].

אנחנו חייבים למצוא איזשהי דרך לוודא שהמידע אכן מגיע אל הצ'יפ שלנו. אבל איך?

[1] מתוך "בשורות טובות" - טרי פראצ'ט וניל גיימן.

לאחר 20-30 ימי משלוח והמתנה של כשעתיים (שהרגישה אינסופית) בסניף הדואר המקומי, התשובה הגיע בקופסא קטנה:

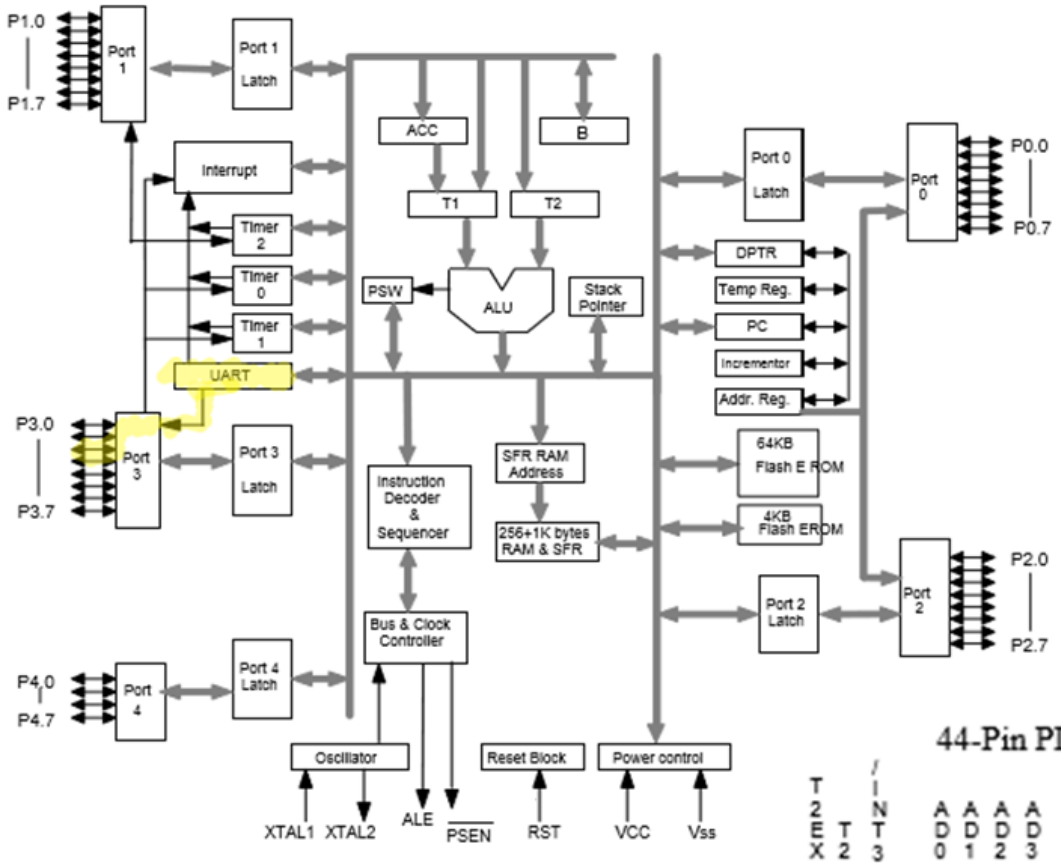
תכירו בבקשה את Logic - Logic-Analyzer מבית היוצר של חברה בשם Saleae.

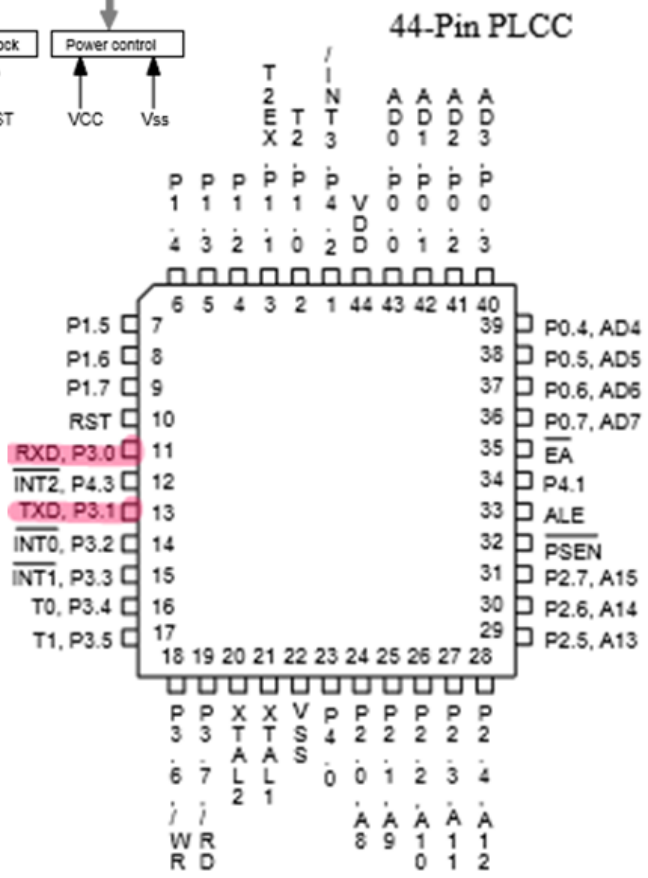
לאלו מכם שלא מכירים Logic-Analyzer, הוא ציוד בדיקה אלקטרוני שמאפשר לחבר תפסים קטנים לנקודת מגע כלשהי במעגל אלקטרוני, ו-"להקליט" את האותות החשמליים שעוברים דרכה. לאחר מכן ניתן לתרגם את האותות האלו למידע בינארי

מצוין, אז בעצם עכשיו אנו יכולים לחבר את LOGIC לרגלי המעבד 8052 שלנו, לבצע שידרוג קושחה מחדש וכך לראות את המידע שנכנס אל תוך המעבד בזמן העידכון.

אבל לאיזה מבין 44 הרגליים של הצ'יפ צריך להתחבר? ואיך בכלל הצ'יפ הזה מתעדכן?

יש רק מקום אחד בו נוכל למצוא את התשובות האלו - חוברת ההגדרות של הצ'יפ, הידועה בדר"כ בשמה הלועזי המקוצר - "Chip Spec":



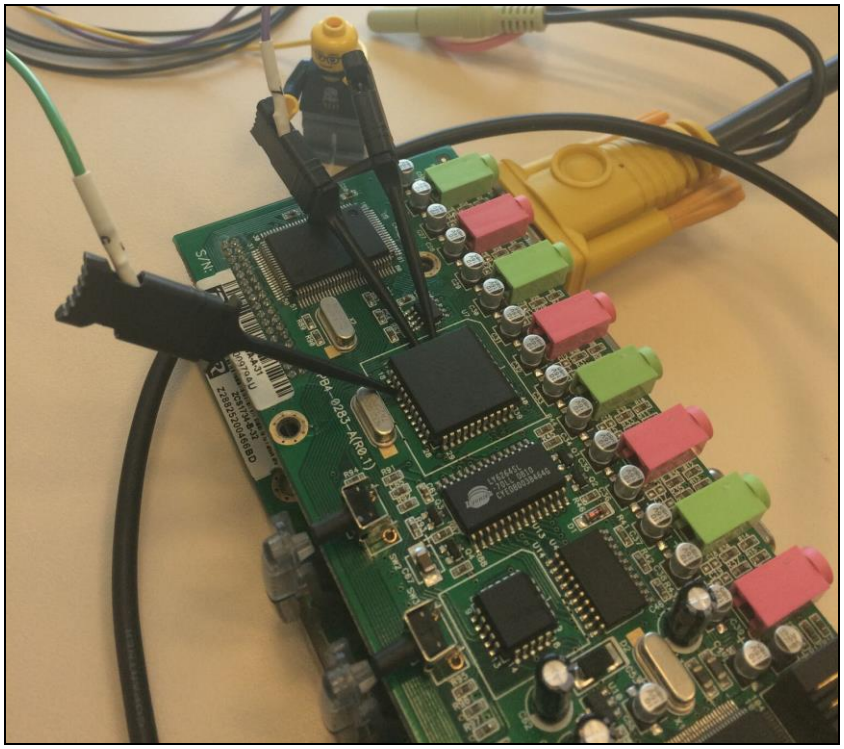


אז מסתבר שלכל מעבד 8051/8052 יש ממשק UART מובנה. לאלו מכם שלא מכירים את המונח UART, מדובר במעין ממשק סיריאלי גנרי "Universal Async Receive Transmit" - שמשמש בעיקר פרוטוקולים כגון RS232 ואחרים.

בצ'יפ הספציפי שלנו ישנן 2 רגליים שמשמשות כ-RX וכ-TX של ממשק ה-UART בזמן העידכון - רגליים מספר 11 ו-13 בהתאמה.

אוקי, אז כל מה שנותר לנו לעשות הוא לחבר את את LOGIC לרגלי ה-UART ולהתחיל להקליט. בזמן שאנו מחברים את הכל ביחד, אנו מתחילים לתהות לגבי התוצאות האפשריות:

- **תוצאה אפשרית מס' 1** - כשלון מוחלט. לא הצלחנו להקליט כלום, או לפחות שום דבר בעל משמעות. זה אומר ששההנחה שלנו היא לחלוטין שגויה והעידכון כלל לא קשור למעבד ה-8052 מה שכנראה יגרום לנו להיכנס לדיכאון עמוק.
- **תוצאה אפשרית מס' 2** - ניצחון מוחלט. איזשהו רכיב אחר בסבך האלקרוניקה שעל הלוח הזה מקבל את ה-BLOB שלנו, מפענח אותו, ואז מעביר אותו מפוענח אל תוך הצ'יפ ואל ממשק ה-UI שלנו.



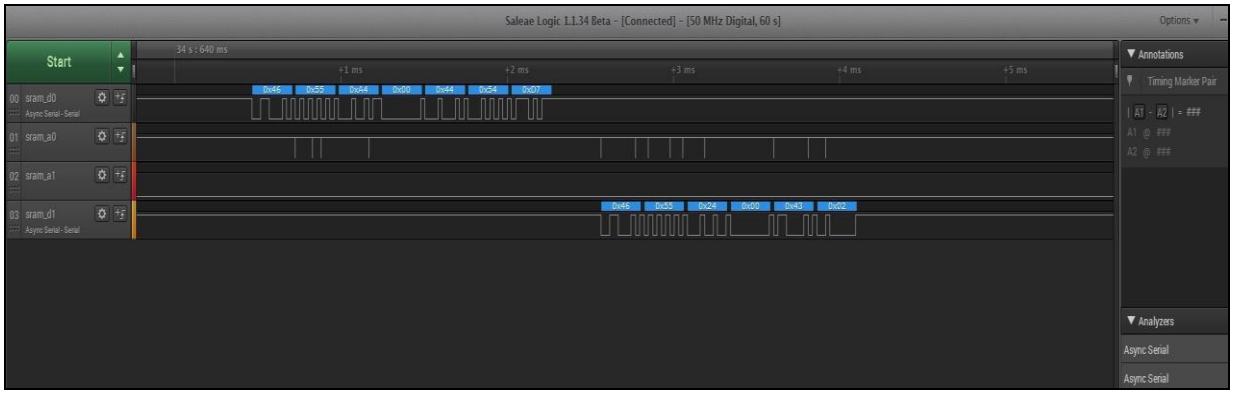
נותר לנו רק לצרוך את מעט האלכוהול שנותר, להחזיק אצבעות ולהתחיל את תהליך העידכון...

זהו, תהליך העידכון הסתיים בהצלחה. אנו טוענים את הכל לתוך ממשק ה-UI של LOGIC, שמאפשר לנתח את ההקלטה. מיד מתגלה לנו תבנית מעניינית.

רגלי ה-RX וה-TX משדרות ומקבלות אותות לסירוגין. נראה ממש כמו פרוטוקול סיראלי .כל שנותר לעשות הוא לנסות ו-"לתרגם" את האותות במודולציה הנכונה. לאחר מספר נסיונות מצאנו את המודולציה המתאימה - Asynchronous Serial - שהיא אחת המודלציות הפשוטות ביותר. עבור כל תקתוק שעון מצב בו יש מתח על הקו מסמן את הביט 1 ומצב בו אין מתח מסמן את הביט 0.

בשלב הבא ניתן להשתמש ב-UI שלנו כדי לתרגם את הביטים האלו לערכי ה-HEX שלהם.

כשמסתכלים על התוצאות שקיבלנו אנו נתקלים ברגשות מעורבים.



מה שאנחנו רואים הוא שבדיוק אותו פרוטורול סיראלי שניתחנו במאמר הראשון הוא זה שמועבר אל תוך הצ'יפ 8052. כלומר, תוכנת העדכון בסה"כ שולחת את כל ה-BLOB דרך הכבל הסיריאלי, ישירות לתוך המעבד. מצד אחד, לא הצלחנו לפענח את ה-BLOB שלנו וככל הנראה הפיענוח מתרחש בתוך הצ'יפ עצמו. מצד שני, עכשיו אנו בטוחים שהצ'יפ שלנו הוא היעד של ה-BLOB וזה אומר שהוא כנראה מתורגם בסופו של דבר לאסמבלי 8051 בדיוק כמו שהנחנו בהתחלה.

עבודה יפה KVM, ניצחת אותנו במערכה נוספת, אבל המלחמה ממשיכה ואנו צוברים יותר יותר ידע בכל שלב !עכשיו כל שנותר לנו לעשות הוא לנסות ולהבין כיצד ה-BLOB שלנו מקודד, ויותר חשוב, איך לקודד אותו בחזרה לאסמבלי 8051 תקין.

המשך יבוא...

נ.ב

עד עכשיו לא ידוע לנו על אף אחד שהצליח לפתור את האתגר שצירפנו למאמר הראשון, פרט לשד טזמני מסוים שעושה רושם שהוא בדרך הנכונה.

אז לצורך החדרת מעט מוטיבציה, אנו מציעים כוס בירה + צ'ייסר חינם לכל מי שיצליח לפתור את האתגר עד לפרסום המאמר האחרון בסידרה. בהצלחה!